University of Alberta

Privacy & the New Panopticon:

Lawful Access and The Race Between Law and Technology in the War on Terror

by

Owen J. Kirkaldy ©

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Laws

Faculty of Law

Edmonton, Alberta
Fall 2008

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-47164-7
Our file Notre référence
ISBN: 978-0-494-47164-7

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Dedication:

This work is dedicated to my wife Jennifer, who met me the day I commenced work on my LL.M. program. She has given me love, support and kindness, and in return I have given her a home-office that looks like a paper mill exploded. This dedication is in thanks for all of the encouragement and support that you have given me since the day we met, four years ago today.

Abstract:

Surveillance and information gathering technology is rapidly outpacing the ability of courts, legislatures and other policymakers to ensure that an appropriate balance is struck between the protection of individual privacy rights and the application of new technology to policing and information-gathering. This paper examines privacy rights in the context of Canada's response to the challenges of terrorism, particularly the proposals for 'Lawful Access' made by the Department of Justice. The courts ought to articulate particular privacy rights that will be protected as opposed to examination of differing means used to invade privacy. The use of the grounds of 'reasonable suspicion' as a basis for invasion of privacy in all but the most marginal of ways ought to be curtailed. An independent body whose role will be to advise Canadians of otherwise secret invasions of their privacy in the course of electronic surveillance should be established.

Table of Contents

1: 1.1 Introduction 1

1.2 Survey of Privacy Law and Legislation in Canada 9

1.3 The Anti-Terrorism Act and how it compares with the reactions to terrorism seen in other jurisdictions 11

1.4 The Current Status of Lawful Access Proposals 15

1.5 Bill C-74 18

2: 2.1 The Definition and Relevance of Terrorism in Canada 24

2.2 The War on Terror – Conflict in Context 31

2.3 What can Canada do to deal with terrorism? 38

3: 3.1 The Definition and Relevance of Privacy in Canada 41

3.2 Competing Conceptions of Privacy in the West 46

3.3 Why Privacy? 50

3.4 Section 8 and Constitutional Protections 56

3.5 Our Privacy Rights 72

4: 4.1 The War on Terror, Reasonable Expectation of Privacy 73

4.2 How Important is Counterterrorism in Comparison to Privacy? 76

4.3 How does a perceived terrorist threat alter the willingness of a society to abandon liberties and alter a Section 1 analysis 84

5: 5.1 Dataveillance and Canadian Society: Tracking Data, the electronic age, and the Panopticon 93

5.2 Is the Reaction against Dataveillance just Paranoia? 94

5.3 Interception of Electronic Mail and monitoring of Internet traffic .. 96

5.4 Electronic Tracking Data collection 103

5.5 Panopticism 105

5.6 The Value of Public Anonymity 114

6: 6.1 Bill C-74 and Proposed Lawful Access Provisions 125

6.2 Adequacy of complaints-driven monitoring of privacy issues 132

6.3 What controls are necessary for Lawful Access to operate safely and effectively? 137

7: 7.1 Conclusion 142

Bibliography 147

Appendix A.. 158

Appendix B.. 159

Appendix C.. 161

1.1 Introduction

On September 11, 2001, the world, or rather the West, experienced a paradigm shift in geopolitical thought in the truest sense of those words. At a stroke, the conception of the global distribution of power as fundamentally being distributed between a collection of nation states was extinguished, and a new conception of the capacity of non-state actors to influence global politics came into sharp focus. Hundreds of millions of people living a largely secular life were drawn - in a matter of seconds - into a previously remote and obscure religious war that they did not understand. Although sub-national Islamist terrorism had been moving from a localized movement to a global anti-American Jihad since the mid 1990s [1], the Millennium was the time that it entered in a serious way into the consciousness of America and the West. As is the case with any truly successful terrorist attack, perception became reality, and overnight the single greatest threat to modern western civilization, in the minds of the public, became Islamist terrorism. Is there truth to the perception? Whether or not there is, what is clear is that the course of history, and the course of legal thought has been changed by these events.

Since 2001, many governments have concentrated state and executive power and expanded the scope of permissible limitation of personal freedoms to a greater extent than has been the case in many years. At the same time as our perceptions of what may be an appropriate level of state and executive authority over individual freedom and privacy has changed, the technology which facilitates the invasion of personal privacy has advanced rapidly and proliferated widely. The technical capacity of state authorities to observe individuals is such today that the possibility exists to remotely log and examine virtually every aspect of any individual life. The need that government feels to employ more and better surveillance technology is partially in response to the use of technology by criminals and terrorists to coordinate action and planning. When measuring the dangers posed by terrorism and the incursion on civil liberties by government, the public must consider that,

---

[1] Gilles Kepel, *The War for Muslim Minds: Islam and the West*, (Cambridge: The Belknap Press of the University of Harvard Press) 2004 at 92-94.

> New technology is not only useful to, and used by, lawbreakers and terrorists, but law enforcement authorities have also increasingly begun to employ such technology (primarily in the form of surveillance technology) in their investigative and enforcement efforts.[2]

Any Western government now has the capacity to realize the most ambitious outcomes of any past police state – that of ensuring that each individual is aware that the state could be observing them at any time.

A race is being run between the capacity of law enforcement and other state agencies to implement technology to monitor individuals and the capacity of the judiciary to interpret technology in the context of civil liberties. This paper will examine the interplay between privacy and security, and make suggestions for how these elements can be balanced in the future, ultimately by changing the rules of the 'race' to eliminate the interplay between increasing technology and judicial interpretation by replacing a technology based interpretation of privacy rights with a principled protection of aspects of individual privacy.

What is needed in order to protect privacy against both public and private sector abuse is privacy law which is based on principle, rather than technology. It is not helpful to have technology-based laws and court decisions which will not give useful guidance once technology changes. It is only by embracing the idea of principle-based privacy protections

---

2 Mary W.S. Wong, "Electronic Surveillance and Privacy in the United States After September 11, 2001: The

that we will have effective privacy laws as well as laws which are predictable from one technological platform to the next. The product cycle of modern information technology is much faster than either the capacity of government to legislate or the capacity of the appellate courts to produce decisions, and as a result, courts and legislators need to look past the technology of the day to the idea which underlies the technology. This is especially relevant as it becomes easier and easier to monitor the typical user's electronic communications, and as personal computers become less stand-alone devices and more Internet portals,

> The rise of always-on broadband has led to a shift towards the use of our personal computers as mere workstations, with private data stored remotely in the hands of third parties. There is little reason to think that people have – or ought to have- any less of a first-order reasonable expectation of privacy for e-mail stored on their behalf by Google and Microsoft than they would have if it were stored "locally" in personal computers after being downloaded and deleted from their e-mail service provider.[3]

This shift places huge amounts of personal data in the hands of third parties, from whom it would be simple to acquire the data without the knowledge of the individual to which it pertains.

Governments pass legislation for the protection of privacy on the one hand, and on the other seek to use technological means to track and monitor their populace. Electronic surveillance and new technologies are at the heart of a rapidly changing area of law, which has huge potential for law enforcement and security, and also for the massive violation of privacy rights. "At a very general level, the law of electronic surveillance recognizes two

---

USA PATRIOT Act" (2002) Singapore Journal of Legal Studies 214 at 215.

[3] Jonathan Zittrain, "Searches and Seizures in a Networked World", (2006) 119 Harvard Law Review Forum 83 at 85.

things: that government surveillance is good, and that it is bad."[4] The ultimate goal of electronic surveillance law must be to maximize the good and minimize the bad.

There has been, in the past several years, an attitude on the part of governments when dealing with terrorism of 'shoot first and ask questions later' which highlights the need for citizens to ensure that their communications and information are not disclosed without oversight and that legal protections for individuals are not discarded in the rush to secure our society from asymmetric political violence. Few people are as familiar with this environment of pre-emption and erring on the side of strong action as Khaled Masri.

> The Masri case, with new details gleaned from interviews with current and former intelligence and diplomatic officials, offers a rare study of how pressure on the CIA to apprehend al Qaeda members after the Sept. 11, 2001, attacks has led in some instances to detention based on thin or speculative evidence. That case also shows how complicated it can be to correct errors in a system built and operated in secret.[5]

Mr. Masri was allegedly abducted by the CIA from Germany, and transported to a third country, believed to be Afghanistan, where he was held for five months for interrogation. This action was based on the fact that his name was similar to that of an associate of a 9/11 hijacker.[6] His story is one of an unaccountable organization abusing its capacity in an overzealous pursuit of its goals. If we are to attempt to ensure that abuses of this scale, or indeed a thousand smaller abuses, do not occur, we must ensure that accountability is built in to our system of security, particularly in the area of surveillance. It is not sufficient for

---

4 Daniel J. Solove, "Reconstructing Electronic Surveillance Law," (2004) 72 George Washington Law Review 1701 at 1704.

[5] Dana Priest, "Wrongful Imprisonment: Anatomy of a CIA Mistake" Washington Post, (4 December 2005), online http://www.washingtonpost.com

[6] Dana Priest, "Wrongful Imprisonment: Anatomy of a CIA Mistake" Washington Post, (4 December 2005), online http://www.washingtonpost.com

government to say that they will exercise their power in a manner consistent with our rights, government must be subject to scrutiny and control where the limitation of rights is involved. Governments in the West, including Canada, have adopted a number of tactics to control terrorism outside of the criminal process, such as immigration policy and no-fly passenger restrictions, which use administrative means to control the movement of individuals deemed to be a risk to society. The difficulty in these cases is that as judicial oversight is generally lacking or reduced, overzealousness results. Some problems arising from, for example no-fly lists, are,

> …potential use of secret evidence… inherent difficulty in proving a negative due to the shift in the presumption of innocence, particularly when one does not know the case against them, and the potential cross-fertilization with other nation's lists, which also renders the decisions potentially unchallengeable in Canada.[7]

Such programs give a preview of how authorization of government surveillance on reduced or eliminated evidentiary requirement might work in practice.

> Canada's Federal Department of Justice has indicated that they intend to lobby Parliament for changes in the law to make it easier for government officials to gain access to data about citizens through a system that they have described in their proposals as 'Lawful Access'[8].

This is a long-overdue policy push, as there is a technological vacuum in which there is a vast amount of information and little direction from courts or legislators as to how investigators ought to treat that data. The difficulty that has arisen in the United States in this regard is that "…it is undertaken entirely in secret, both as a general matter and for any specific search, and it exists in the absence of any statutory framework or judicial oversight."[9] It is this difficulty that the imposition of rules regarding such matters as electronic tracking data could avoid. These proposals would affect individual privacy in many ways. They would ease the requirements for access to electronic data about an individual, in particular information about electronic transmission of information, and would allow the government to gain so called 'tracking information'[10] such as records of debit card transactions and cell phone, personal data assistant, and automobile GPS locations, on a 'reasonable grounds to suspect' basis, even though this information discloses a large amount of private information about an individual - potentially dangerous information if an individual unwittingly converses *or* corresponds with a terrorism suspect. It would also allow for the production of information from Telecommunication Service Providers (TSPs) on a lower evidentiary burden than is currently the case. This has caused a great deal of comment from privacy advocates around the country, both privately and from government privacy commissions, with good reason. A great deal of information about the individual will be under closer and less regulated scrutiny under this proposed regime than before, with little justification of the necessity of such measures.

---

[7] Faisal Kutty & Arsalan Dhirazi, "Canada's Passenger Protect Program: Too Guilty to Fly, Too Innocent to Charge?" Submission by the Canadian Council on American Islamic Relations (CAIR-CAN) on Passenger Protect Program: Identity Screening Regulations to transport Canada, January 31, 2007, online http://ssrn.com/abstract=962797. At 22.

[8] Department of Justice Canada "Lawful Access: Legal Review Follow up consultations: Criminal Code Draft Proposals February-March 2005." http://www.cippic.ca/uploads/JC_CCAmend_2.pdf

This paper will examine the threat posed to Canada by terrorism, the importance of privacy in our society, the merits of trading privacy for security from terrorism, the potential for technology to fundamentally alter the nature of privacy invasion, and how we can protect our privacy, while still ensuring that appropriate tools are in place to allow law enforcement to investigate crimes which are planned and even carried out through an electronic medium.

Part one of this paper will discuss the legislative background of privacy in Canada, the aspects of the Anti-terrorism Act that affect privacy, the proposals set out by the Canadian federal Department of Justice relating to 'Lawful Access' and the current status of those proposals, and a brief comparison of anti-terrorism acts in the United Kingdom, United States and Canada. The second part of this paper will examine the War on Terror and terrorism from a Canadian perspective, and will draw the conclusion that terrorism, while it is a concern to be addressed, is not the most pressing or substantial threat to Canada. The third part of this paper will examine the nature of privacy as interpreted in Canada and Canadian constitutional protections of privacy, and will include a discussion of the application of section 8 of the Charter of Rights and Freedoms[11] to the invasion of privacy by government authorities. The fourth part of this paper will examine a constitutional analysis of terrorism prevention measures effect on privacy and the relative importance of terrorism prevention and privacy and whether anti terrorism is of sufficient importance to justify the negative effects on personal liberty brought about by proposed Lawful Access provisions. The fifth part of this paper will examine panopticism and surveillance and how it should be controlled in Canadian society. It will be argued that whether or not panoptic data surveillance, or dataveillance, is accepted by the courts as falling in line with the Constitution, that for policy reasons, it ought not to be implemented. Part six of this paper will deal with specific proposals made regarding the implementation of early portions of Lawful Access provisions through the introduction in the 38th parliament of Bill C-74.[12] Finally the conclusion of this paper will make recommendations for how best to protect privacy in the face of the need for a regime surrounding the use and collection of information generated by technology in our society, including the abandonment of the reasonable suspicion standard for applications for information under all but the most limited Lawful Access provisions, the creation of a body whose role will be the mandatory reporting to individuals that they have been targeted by Lawful Access investigations, and the application of a principled approach to the protection of privacy which sets out precisely what kinds of private information we will allow to be invaded based on reasonable suspicion and which we will require a higher standard in order to gain access.

---

[9] Jonathan Zittrain, "Searches and Seizures in a Networked World", (2006) 119 Harvard Law Review Forum 83at 91.

[10] Tracking information pertaining to Lawful Access proposals differs from a tracking warrant. A tracking warrant under s. 492.1 of the Criminal Code provides for a warrant on the basis of 'reasonable suspicion' to be granted, on application, for a period of 60 days for monitoring and installation of a device to track the location of an individual or thing. A tracking data warrant would be for a period o one year and would permit the collection of all an individual's tracking information provided by such devices as GPS, RFID, e-mail, Banking and Credit cards, and other forms of location.

---

[11] *Canadian Charter of Rights and Freedoms* Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.).

[12] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information,* 1st Sess., 38th Parl., 2005, (1st

---

reading 15 November, 2005).

1.2 Survey of Privacy Law and Legislation in Canada

There has been growing concern for the protection of privacy in Canada in recent years. Legislation has been enacted for the purpose of privacy protection, [13] and privacy watchdogs have been established,[14] while at the same time, the means that are available for the purposes of collection of private information and the interpretation of that information through electronic means have grown exponentially. Awareness of privacy has grown, and as a result, government has been willing to act to protect privacy.

The main thrust of protection of privacy in Canada as it relates to legislation affecting the government has been to prevent the collection, use or disclosure of personal information by the government except as permitted by express or implied consent,[15] and in defining what makes up personal information.[16] These pieces of legislation have also provided for the implementation of watchdog organizations in the form of the privacy commissions, which have the role of investigating complaints pursuant to privacy legislation and pursuing litigation where necessary to ensure compliance with privacy legislation. Privacy commissioners also have a role in the promotion of awareness of privacy issues with the general public. It is generally not the normal day-to-day collection and interpretation of information by government, however, that causes concern in the context of the protection of Canada from terrorist threats.

Privacy concerns become more complex where they begin to overlap with criminal law investigative powers of search and seizure and the liberties ensured by Section 8 of the

---

[13] For Example, *Privacy Act* R.S.C. 1985 c. p-21, *Freedom of Information and Protection of Privacy Act* R.S.A. 2000 c. f-25,

[14] *Privacy Act* R.S.C. 1985 c. p-21 s. 53-54.

[15] *Privacy Act* R.S.C. 1985 c. p-21 s. 2. See appendix C.

[16] *Freedom of Information and Protection of Privacy Act* R.S.A. 2000 c. f-25, s. 1 (n), see appendix C.

Charter of Rights and Freedoms.[17] A more complete examination of the application of Charter rights to privacy protections enshrined by S. 8 of the Charter of Rights is found in Sections 3 and 4 of this paper. Privacy as set out in privacy legislation is not the focus of this paper, except insofar as the existence of a privacy framework in Canada shows that privacy is valued as a right and there is an expectation outside of bare constitutional norms that government will protect the privacy of individuals from invasion by the state.

---

[17] *Canadian Charter of Rights and Freedoms* Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.).

1.3 The Anti-Terrorism Act and how it compares with the reactions to terrorism seen in other jurisdictions

Where privacy is to be analyzed in the context of Canada's response to terrorism, we must review what that reaction has been. We may also wish to examine how Canada's reaction has compared with that of its allies. The initial response to terrorism adopted in Canada after the attacks of September 11, 2001 came in the form of Bill c-36, now commonly called the Anti-terrorism Act.[18] This legislation was brought forward very shortly after the attacks and represented the implementation of a broad range of legislative provisions. Several amendments were made to the Criminal Code, including a section defining terrorism broadly, with a requirement that a terrorist activity be motivated for a political, religious, or ideological purpose.[19] The definition has been criticized for adding nothing to the law, but instead adding a new and more difficult way to prosecute old crimes such as conspiracy to commit murder.

Other aspects of the act include provisions for investigative hearings which would compel individuals to provide testimony without the option of remaining silent,[20] as well as provisions allowing for arrest without warrant and the holding of an individual without judicial authorization for up to 24 hours.[21] These provisions were subject to a sunset clause requiring review and re-approval by parliament in late 2006. The sunset clause took effect, and these provisions are no longer with us. There was widespread concern about the effectiveness of these provisions and the need for exceptional powers, and even their usefulness in preventing terrorism. Further, the use of motive as a portion of the definition of terrorism has been successfully challenged through Canadian courts, and that portion of the definition has been struck down, leaving little to the residual definition of terrorism in Canada.[22] The immediate reaction bought about by the Anti-terrorism act has, in great measure, gone by the wayside through sunset provisions and constitutional challenges. What has remained unchanged is the belief in many quarters that terrorism is the main threat to Canada today, a notion that is contested in latter sections of this paper.

---

[18] *Anti-terrorism Act* S.C. 2001 c. 41.

[19] *Criminal Code* R.S.C. 1985, c. C-46, s. 83.01 (see appendix c)

The United Kingdom, unlike Canada, has had a long and tragic history of dealing with terrorism in the form of violence in Northern Ireland. As such, the UK had already in place anti-terrorism measures when Canada passed its Anti-terrorism act, and had revised it as recently as 2000. The *Terrorism Act 2000* [23] Which defined terrorism broadly, as broadly as in Canada, and including a motive element, and expanding powers of search and detention beyond those permitted by those in the Canadian Anti-terrorism act. The UK act allows for arrest based on 'reasonable suspicion' without warrant, and the holding of a suspect for up to 48 hours without hearing.[24] In some cases an individual may be held for longer without charge. The United Kingdom has felt a much greater burden of terrorism throughout the last several decades, and as such there seems to be a much greater willingness on their part to abridge liberties than in Canada.

In the United States, the PATRIOT Act was the main legislative response to September 11.[25] While the PATRIOT act covered a broad range of topics, like other acts it enhanced investigative powers and sought to compel the production of private information

---

20 *Criminal Code* R.S.C. 1985, c. C-46 s. 83.28 (see appendix c)
21 *Criminal Code* R.S.C. 1985, c. C-46 s. 83.3. (see appendix c)
22 Khawaja v. the Queen, 2006 O.J. no. 425 SCJ.
23 *Terrorsm Act* (U.K.), 2000, c 11.
24 *Terrorsm Act* (U.K.), 2000, c 11. s. 41(3). (see appendix c)
25 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* Pub. L. No. 107-56, 115 Stat. 272 (2001).

in the absence of judicial authorization. Title V to the Patriot Act provided for the issuance of 'National Security Letters' which would require the secret provision of information by an organization served with such a letter. A gag order concealed the existence of such a letter. This measure, providing for the secret collection of information without the possibility of making a legal challenge was struck down as unconstitutional by the courts in the United States.[26] Other privacy issues raised in the PATRIOT act include clarifications of how electronic communications are to be intercepted, [27] broadening the types of subscriber information that law enforcement can obtain from service providers (much like the provisions of Bill c-74 would have done)[28] And expands the authority to apply 'pen register' and 'trap and trace'[29] rules to Internet and other electronic transmissions,[30] much as Lawful Access provisions recommended under proposals on transmission data. Like it did in Canada, the anti-terrorism legislation in the United States contained significant sunset clauses, but unlike in Canada, much of the PATRIOT act provisions were reinstated after the sunset period.

To summarize the comparison of American, British and Canadian anti-terrorism legislation, we see that Canada's is likely the least rigorous, while the detention clauses in the UK legislation are harsh enough that Canada did not re-enact much less stringent rules surrounding arrest without warrant. In the United States, the breadth of the PATRIOT act dwarfs the legislative reaction in Canada, but parallels some of what was done, and foreshadows much of what has been proposed through Lawful Access. The PATRIOT act has pointed he way for much of the Lawful Access regime proposed by the Department of Justice, particularly in the area of production orders for transmission data. All the legislation contains elements designed to attack terrorist funding and money laundering. Canada's response to terrorism has been relatively restrained, and the stalling of the process of moving forward with Lawful Access has shown that there is little political will to create new security provisions without some new emergency creating an air of urgency.

---

[26] *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

[27] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* Pub. L. No. 107-56, 115 Stat. 272 (2001). S. 209.

[28] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* Pub. L. No. 107-56, 115 Stat. 272 (2001).s. 210.

[29] Pen Register and Trap and Trace are terms referring to what in Canada would be referred to as DNR, or Dialed Number Recorder, providing telephone routing information.

[30] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* Pub. L. No. 107-56, 115 Stat. 272 (2001). S. 216.

1.4 The Current Status of Lawful Access Proposals

Lawful Access is a term used by the Department of Justice in Canada to refer to a set of proposals brought out in the wake of the September 11 attacks which were designed to allow for enhanced monitoring of individuals through electronic means. Highlights of these proposals include the creation of two new production orders, one for 'tracking information'[31] and 'transmission data'[32] based on a 'reasonable grounds to suspect' criteria, and extending those orders from sixty days to one year, expanding the application of tracking warrants to include GPS or other location devices carried willingly by a suspect, without the necessity of implanting a device for tracking as well as including debit and credit card transactions in a tracking warrant, to expand DNR Warrants[33] to cover all transmissions on the Internet or any other means of communication, the creation of 'preservation orders' which would be used by aw enforcement without judicial authorization to order the custodian of information not to delete that information, and allowing for terms in a preservation order to prevent disclosure of the order, and for an order requiring a telecommunications service provider to disclose information about its subscribers without the necessity of a court order.

---

[31] information that would assist in determining the location of a person or thing at a particular time, Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations:Criminal Cose Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic online http://www.cippic.ca/en/projects-cases/lawful-access/ at 19

[32] data relating to the telecommunications functions of dialing, routing, addressing or signaling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility. Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations:Criminal Cose Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic online http://www.cippic.ca/en/projects-cases/lawful-access/ at 21.

[33] *Criminal Code* R.S.C. 1985, c. C-46, s. 492.2 (see appendix c)

How will implementing Lawful Access change Canadian law as it stands today? First, there would be a massive expansion of the information that authorities could collect based on 'reasonable suspicion' both by conscripting the suspects personal electronics and use of telecommunications, but also by making the application of those warrants retroactive. Currently, if a tracking warrant is granted, a tracking device must be installed. Likewise for a DNR warrant. By adding electronic records to the means used to acquire this information, they are not necessarily prospective in nature, and can collect information gathered by electronic means prior to the raising of even reasonable suspicion and the application for the order. By expanding the types of information and manner in which information is collected pursuant to production orders, and extending the duration of those orders from a maximum of sixty days without further judicial intervention to one year, the level of invasion of privacy experienced by the subject of such an order is increased tremendously.

Other aspects of the proposals are not as troubling, such as the issuance of a preservation order by law enforcement officials. It is extremely easy for electronic information to be deleted, and it is not unreasonable for a mechanism to be put in place to permit authorities time to seek a warrant for production of suspect information. The production of subscriber information without judicial supervision is somewhat problematic, although there are circumstances, particularly in the prosecution of online child exploitation, that a reasonable necessity for instant access to such information exists.

The first attempt to implement any of the proposals brought forward by the Lawful Access provisions was bill C-74[34] in late 2005. That bill would have provided for the disclosure of subscriber information on the request of an authorized police officer[35] and required the creation by telecommunications service providers of a system permitting government to acquire information from their data networks, thus forcing the private sector to build and pay for law enforcement tools within their systems which would permit the disclosure of private information without judicial authorization. This piece of legislation only received first reading by the time parliament was dissolved for an election. Since that time, notwithstanding the interest that the Conservative government has shown in issues of security, little has been done to revive these proposals. The difficulty that arises is that until the proposals are adequately dealt with, there is no legislative framework in place to govern the production and use of a broad variety of data, and while it may not be advisable to implement the proposals as drafted, some sort of principled approach to the implementation of electronic data monitoring is desirable.

---

[34] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications*

---

subscriber information, 1st Sess., 38th Parl., 2005, (1st reading 15 November, 2005).

[35] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information,* 1st Sess., 38th Parl., 2005, (1st reading 15 November, 2005), s. 17.(see appendix c)

1.5 Bill C-74

On November 15, 2005, even as the Liberal government was on the verge of an election, Bill C-74[36], The Modernization of Investigative Techniques Act, was introduced at first reading. The stated goal of the bill was to require telecommunications service providers to facilitate interception of communications and to provide subscriber information to the authorities. Although this legislation did not advance in the form of Bill C-74 due to a change in government, its key points were taken directly from the Lawful Access proposals, which set out the Department of Justice's perceived needs for revitalizing the abilities of authorities to deal with increasingly technology savvy criminals. While we may never see this bill in Parliament again, its underlying motivations – those of dealing with advancing technology in the context of criminal investigation and establishing rules for surveillance of the Internet and telecommunications – remain as top priorities in this country. This bill does not significantly extend interception or tracking powers, rather as a preliminary matter it requires telecommunication providers to build in a technical capacity for the authorities to access telecommunications information, laying the framework for future interception regulations and laws, and establishing responsibility squarely with service providers for the construction of a surveillance system on a grand scale never before seen for use on the Canadian public.[37]

Bill C-74 also establishes a requirement for TSPs to provide "subscriber information" such as address, name and location when requested to do so by a peace officer or CSIS agent.[38] This would give the police the power to, for example, acquire the name, address, and other contact information of an individual based on his or her instant message signature or e-mail address. This power would be exercised without judicial authorization, and monitoring would be minimal.[39] The only monitoring provided for in this section is self-enforcing, with little oversight by any parliamentary or judicial authority. Those requesting information would be required to create a written record regarding the request for the information, there would be no capacity for the person so investigated to become aware of, and therefore object to, the provision of the data. This provision is much akin to requiring the establishment of a reverse-directory for Internet applications, which in and of itself is not likely to lead to excessive concerns over privacy issues, especially if users are aware of the information which is liable to be disclosed. This tool is liable to be especially useful in searching for Internet child predators, who use instant message technology to lure children for sexual purposes. Again, however, the transparency of this provision ought to be enhanced through the use of mandatory disclosure to the subject of the information request after a certain period of time unless it can be reasonably justified that there is a pressing need to maintain secrecy. A third-party watchdog organization reviewing the written records already provided for in this section and ensuring that the public was aware of information requests made about them would be beneficial. The privacy invasions contemplated are too important to go un-monitored, an audit function must be included in developing access legislation.[40] If a person is being investigated, the fact of the investigation and the reason for it ought to be made available to them subsequent to the investigation in order to prevent abuse. Furthermore, to ensure that the public was aware

---

[36] Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, (1st Reading 15 November 2005).

[37] Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, (1st Reading 15 November 2005). S. 11. (see appendix c)

[38] Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, (1st Reading 15

November 2005).

[39] Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, (1st Reading 15 November 2005).

40 Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", (2008) 75 University of Chicago Law Review 261 at 269.

of information requests made about them, the use of this tool in a 'fishing expedition' manner or for other inappropriate purposes could be discouraged.

One issue to be dealt with in this respect is the continuing utility of the Internet after the development of enhanced monitoring by the government. It is relevant to note that a large part of the appeal of the Internet has been the sense of anonymity that it gives to its users. Just as traditional mail has developed in a particular way because of the certainty of privacy on the part of its users, the Internet and e-mail have developed in a certain way and have expressed a certain kind of social utility based on its anonymity. The very nature of a typical e-mail address,[41] often a pseudonym which does not describe the user in any identifying detail and omitting proper names[42], indicates that a certain type of obscurity is desired by Internet users. The Internet is a marketplace of ideas and a forum for rapid and universal communication. It is a forum where one feels free to express thought and opinion without fear that such expression will be connected to one's physical self. This providing a reverse directory application for Internet screen names and e-mail addresses which can link a person to their physical location weakens that role of the Internet as an anonymity granting social phenomenon. It is therefore important that the general public not have access to any information system established by law to allow for policing. The social utility of the Internet will be fundamentally altered if this provision leads to the establishment of a published equivalent to a reverse telephone directory. It would be more than sufficient in order to help prevent criminal abuse of the Internet to maintain a capacity for law enforcement to backtrack to a user based on identifying information in limited circumstances.

---

[41] Particularly those chosen by the user, rather than assigned by an institution.

42 Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging

Likewise, by tracing IP addresses, the anonymity of web 'surfing' is lessened. The Internet has created a vast network of informational pages on a variety of topics ranging from academia to medical diagnosis, to the less savory areas of drug subculture and hard core pornography. It has also acted as a catalyst for social activism and the proliferation of an alternative media, through the use of e-zines and blogs to distribute first-hand reports of news events. These have had a mixed effect, providing for the growth of alternative viewpoints and creating a virtual space in which developing social ideas can grow, but they have also demonstrated that the law has lagged behind technology. Take as an example the violation of a publication ban during testimony of the Gomery Inquiry in 2005.[43] At that time, a judicial inquiry operating under a publication ban partially lifted the ban due to the fact that firsthand accounts of testimony had been published on an American Internet site, and that maintaining the ban was becoming increasingly difficult.[44] Take as another example the use of the Internet, cell phones, mobile e-mail devices and the like to co-ordinate mass public demonstrations. By providing instant mobile communication which can be sent to dozens or hundreds of people at once, mobile communications technology has allowed public protests a degree of organization and continuing communication which was previously available only to the authorities operating to control the crowds. In these cases, technology has advanced beyond control of the authorities. Clearly there is a need for an update of Canada's laws surrounding technology and

---

Regulatory and Technological Approaches", (2008) 75 University of Chicago Law Review 261 at 277.

[43] In 2005, during the inquiry of Justice John Gomery into the use of federal funds to purchase federalist advertising through agencies friendly to the Liberal Party, an American Internet site violated the publication ban that was in place, thereby circumventing the publication ban and making the restricted information available in Canada. The Justice responded by partially lifting the ban.

[44] Rondi Adamson, "Borderless Blogs vs. Canada Press Ban," Christian Science Monitor, April 13, 2005. online, http://www.csmonitor.com.

communication. Such electronic crimes as e-mail fraud,[45] spamming, DNS[46] attacks, and hacking have demonstrated a need for the Internet to be monitored more closely, especially as so much of the commerce of the developed world now relies heavily on the instant communication of the Internet, but it must not be at the cost of the social utility which has accompanied the economic gains allowed through technology.

The main danger of the provisions set forth in Bill C-74 is that of laying an unobtrusive groundwork for an unprecedented electronic monitoring system. What is liable to come after is much more invasive than what has already been proposed in Parliament. It is well worth noting that had all of the provisions of the Lawful Access proposals been put forward in an omnibus bill, the attention drawn would have likely been much greater. By establishing the technical requirements first, there is the potential to bring forward in palatable bites what might not be swallowed by the public in whole form.

There has already been a groundwork laid providing for a requirement for uncompensated provision of information pursuant to production orders on ex-parte application.[47] Financial compensation is not required where telecommunications service providers or others incur expense in compliance with a production order under the Criminal Code of Canada. The remedy where costs of compliance would be so financially burdensome on the subject of the production order that the results would be unreasonable is an exemption from production.[48] While this may not be a concern where Telus is the subject of a production order, there are a large number of small service providers whose resources might make it more difficult to enforce production. This would appear to be a major factor in the requirement under C-74 to install easy to use backdoor systems for the collection and production of information useful to investigators. By front-loading the expense of future production orders by requiring the installation of such a means of collection of information at the time of a system upgrade, the government is seeking to side-step the potential pitfalls of the Telus decision and eliminate the possibility that any particular production order might be subject to an exemption.

---

[45] Sometimes called "phishing", where a fraudulent but official looking e-mail is sent, allegedly from an institution, requesting the confirmation or disclosure of personal information for the purposes of identity theft or credit or bank fraud.

[46] Denial of Service Attacks, in which a website is targeted for excessive traffic, causing a temporary shutdown, which may lead to public embarrassment or loss of business.

47 *Criminal Code*, R.S.C. 1985, c, C-46 s. 487.012.

48 *Tele-Mobile Company (a.k.a. Telus Mobility)* v. *Ontario*, [2008] SCC 12.

2.1 The Definition of Terrorism in Canada

There is a great deal of debate surrounding the definition of terrorism. Much of this debate stems from the virtual impossibility of creating a definition that will include all perceived terrorist actions, while excluding all perceived non-terrorist actions. This problem has essentially prevented an international treaty definition of terrorism, because terrorism is, to a great extent, a crime of perception. Arguments of justification on behalf of liberation movements and so-called freedom fighters, and differing perceptions of the possibility of limiting civilian casualties in any conflict tend to stymie debate on a broadly applicable definition.[49] For the purposes of combating terrorism from a local standpoint, however, any sufficiently broad definition of terrorism will work to some extent. Canada's very broad definition allows for the prosecution of a vast array of offences under our terrorism laws, while the requirement for political oversight[50] theoretically prevents overzealousness on the part of local law enforcement officials in using these powerful laws against otherwise non-terrorist criminal elements. In spite of arguments that it is inappropriate to include such a wide and subjective definition of terrorism, and one which is dependent on political approval, so long as its application to other legislation does not cause that legislation to overreach its rational purpose this broad definition may well be sufficient in the Canadian context considering that the search for a more specific definition of terrorism which can cross cultural and political boundaries has gone on for decades.

---

49 Malvina Halberstam, "The Evolution of the United Nations Position on Terrorism: From Exempting National Liberation Movements to Criminalizing Terrorism Wherever and by Whomever Committed", (2003) 41Columbia Journal of International Law, no. 3 p. 573 at 576.

[50] *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.28(3) and s. 83.3(1).

The history of asymmetric political violence is a path littered with the most idealistic concerns for the improvement of society,[51] and the most political and cynical ambitions for self advancement. It is likely not possible to arrive at a single definition of terrorism agreed upon by a wide enough cross section of the global community to be useful, in large part because of the old saw, "One man's terrorist is another man's freedom fighter." Each involved party will attempt to define terrorism so as to exclude themselves and to include their opponents. Especially at the United Nations, the prevalence of states which have gained independence through asymmetric political violence muddies the issue to the point where terrorism is legitimized in the context of war for self-determination. In the 1970s, as modern international terrorism was experiencing a wave of media attention and rising to prominence on the minds of many throughout the world, both inside and outside the political world, the General Assembly adopted an early resolution condemning terrorism but, "[reaffirming] the inalienable right to self-determination and independence of all peoples under colonial and racist regimes and other forms of alien domination and upholds the legitimacy of their struggle, in particular the struggle of national liberation movements."[52] The wording of such resolutions, failing to condemn terrorism in all situations can be viewed as excusing national liberation groups from the UN anti-terrorist stance.[53] The inclusion or exclusion of the state use of terror, the requirement for certain types of motivations, the protection of revolutionary armed groups engaged in struggle against particular governments or states from the terrorist label are all concerns which prevent a meaningful resolution to the question of what the term terrorism actually means.

---

[51] For example the resistance to Nazi occupation in Europe during the Second World War, or the fight against Apartheid by the ANC.

52 "Measures to Prevent International Terrorism which Endangers or Takes Innocent Human Life or Jeopardizes Fundamental Freedoms, and Study of the Underlying Causes of those Forms of Terrorism and Acts of Violence Which Lie in Misery, Frustration, Grievance and Despair and which Cause Some People to Sacrifice Human Lives, Including Their Own, in an Attempt to Effect Radical Changes" G.A res 27/3034, UN GAOR, 27th Sess., Supp No. 30 at 119, U.N. Doc A/RES/27/3034 (1972)

53 Malvina Halberstam, "The Evolution of the United Nations Position on Terrorism: From Exempting National Liberation Movements to Criminalizing Terrorism Wherever and by Whomever Committed", (2003) 41Columbia Journal of International Law, no. 3 p. 573 at 575.

From a Canadian perspective, however, it is immaterial whether there can be broad international agreement on the definition of terrorism, so long as consensus can be attained within a Canadian context. Most Canadians would agree that a non-state individual or group using violence against civilians in order to achieve a political goal ought to be at least *included* in the definition of terrorism, even if that definition is not exclusive of other potential meanings. This paper will use this definition unless otherwise indicated and will reject the inclusion of the overt acts of any state or its publicly acknowledged official agents in the definition of terrorism[54]. Acts such as aerial bombing, massacres of civilians by government forces and forced relocation of populations, while all may be designed to cause fear in opposing civilian populations, are all acts of the state and are covered by existing international law. Those who engage illegally in these acts are properly war criminals, not terrorists. Acts of recognized state agents such as intelligence agencies, while they may be in form similar to, or even indistinguishable from acts of terrorism, are conducted by or on behalf of a state, and these actions are subject to an extant body of international law which condemns the use of force by states or their agents under most circumstances and outside of tightly prescribed conditions.[55] Where states or their overt agents engage in war crimes or crimes against humanity, they ought to receive appropriate

---

[54] For example, I would not describe the assassination of a civilian by the secret service of a state in order to bring about a change of government in a third state as terrorism, as it is carried out by an acknowledged official arm of government. An individual belonging to a non-state group who committed the same act might, however be guilty of terrorism. In the case of such groups as Hezbollah, who are allegedly funded and largely directed by the government of Iran, but are not an acknowledged arm of that government, it would also be defined as terrorism. The purpose of exclusion under this definition is to exclude the overt acts of states from consideration as terrorist acts, as these acts are already regulated under existing bodies of established international law.

55 Whether there is an effective enforcement mechanism or not for international cranial law is a matter outside the scope of this paper. It is sufficient for these purposes to be aware that a new area of international

sanctions under extant international law. To describe these actions as terrorism, however, leads to an imprecision in our language as a result of rhetorical usage to denounce a political regime with which one disagrees. This does not help to advance the cause of promotion of the rule of law, rather it only results in increased vitriol between those who use this terminology and those with whom they label it. It is not useful to attempt to broaden the definition of terrorism to include an entire category of already denounced illegal activity by drawing parallels between the illegal acts of states and non-states.

The greater difficulty with the definition of terrorism within Canada's Anti-Terrorism Act is its breadth and the discretion allocated to the minister regarding prosecutions and the listing of organizations as terrorist groups. The definition of terrorism used in the Anti-Terrorism Act has been criticized for over breadth,[56] these criticisms stemming from the fact that the definition leaves room for an incredible array of crimes to be transformed into terrorist crimes based on a motivational political or religious element. The preventative measure which is used to ensure that there will be no inappropriate prosecutions is the requirement of consent of the attorney general to any prosecution which is commenced. This leaves the definition of terrorism as whatever the cabinet decides is terrorism, and perfectly illustrates the problems facing citizens where terrorism is concerned. The difficulty this creates is an imbalance between the executive-legislative branch of government, and the judicial branch. The "we know terrorism when we see it" outlook taken by the government does not allow for predictability in relation to whether one is or is not involved in terrorist activity. The requirement that we as citizens trust implicitly in the wisdom and even-handedness of our executive branch of government does

---

law does not need to be established in order to deal with state actions.

[56] See for example, Kent Roach, *September 11: Consequences for Canada*, (Montreal: McGill – Queen's

not coexist happily with our conception of the rule of law and constitutionalism. This problem has been recognized and partly dealt with in the Ontario Superior Court of Justice, which recently struck down the motivation requirements of the definition of terrorism.[57] The issue identified as fatal to the definition was the potential chilling and discriminatory effect of focusing the power of criminal law on political, religious, and ideological thought, and the discrimination that would inevitably occur in the enforcement and investigation of these laws.

Western strategic thinkers were so focused on state to state interactions during the cold war era that the notion that non-state-sponsored terrorism was simply not at the forefront of concern. The West could not conceive of a substantial threat to its well being coming from a non-state actor.[58] The inability to come to terms with sub-state level violence is likely one of the causes of the state-level interventions in Afghanistan and Iraq. Unfortunately, through aggressive military campaigning in the Middle East in Iraq and Afghanistan, we seek to treat the symptom rather than the cause of terrorism, and in doing so, may create conditions which will lead to terrorism in the future. Anti-terrorism measures are creating animosities which will take lifetimes to dissipate. The result of this is that domestic anti-terrorism measures will be perpetuated in a continuing environment of pseudo-warfare, in which a war-like situation is cited as cause to continue policies which limit our natural and hard-won freedoms. During an extended pseudo-war period, the executive branch of government will continue to seek to exercise wartime powers and increase their security related capacities at the expense of civil rights. Should this continue

---

University Press, 2003.) pp. 56-64.

[57] Khawaja v. the Queen, 2006 O.J. no. 425 SCJ.

[58] See, for example, the analysis of Islamic Fundamentalist threats in Graham E Fuller, "Islamic Fundamentalism", in *Conflict After the Cold War: Arguments on Causes of War and Peace*, Richard K. Betts ed. (Boston: Allyn and Bacon) 1994, 386-393 at 390-391.

indefinitely, we will see serious damage to our way of life. In the case of War on Terror, there is no foreseeable end point, there is no practical way of achieving victory, and there is no limit to the level of expenditure of treasure, political capital, and freedom which can be made to ensure the possibility of a successful outcome.

Just a few months after the September 11 attacks, cooler heads were promoting the importance of ensuring the continuation of liberty in the face of adversity in order to reinforce the legitimacy of the struggle in favour of the West. David Cole wrote in 2003 regarding the importance of ensuring legal protection for not just citizens but foreign nationals,

> [to only apply human rights standards to citizens] is counter-productive as a security matter. Counter productive it seems to me because it forfeits the legitimacy of the War on Terrorism. If we are to win the War on Terrorism, we need to be seen as acting in a legitimate and justice seeking mode. Not in a double standard mode that says we are willing to impose on you foreigner things we are not willing to tolerate for ourselves. That undermines the credibility of the effort and that then has two pernicious effects. First, it alienates the very communities that we need most to be building bridges to if we are to try to find the small numbers of Al Qaeda people out there… Finally, it is illusory, because if you look at history, indeed, even recent history, what starts with foreign nationals almost inevitably gets extended to US citizens.[59]

It is promising, however, that after a number of years of moving towards trading freedom for security, many are questioning the reasonableness of so doing. In America, but also in other states including Canada and Great Britain, security measures have been taken which many find incompatible with their perception of a free society, and many are willing to begin to oppose those measures without fearing being labeled a friend to terrorists or unpatriotic. Through this re-balancing we may find an appropriate balance of security and

---

59 David D. Cole, "Security and Freedom – Are the Governments' Efforts to Deal With Terrorism Violative

civil rights. Examples like Maher Arar[60] and Khaled Masri are causing many to believe that secrecy and unaccountability are dangerous tools in the hands of even the best intentioned patriots, and that some form of protection from overzealousness is necessary in any case where secrecy and the power to sanction and detain overlap.

---

of Our Freedoms?" (2003) 29 Canada-United States Law Journal, 339 at 343.

[60] Maher Arar was a Canadian citizen who was detained when passing through American customs based on very little evidence, and who was ultimately transported to Syria and tortured to extract information about terrorism – information which Mr. Arar did not have.

2.2 The War on Terror – Conflict in Context

One way in which encroachments on privacy are justified is through the rhetoric of war used in relation to terrorism. The War on Terror is not like other wars in a number of ways. Many have commented on its potentially indefinite duration, thus bringing into question the viability of utilizing wartime measures in its prosecution. Others have commented on the issue of whether it is properly a war at all.[61] Wesley Pue described the difficulty of the war metaphor for counterterrorism succinctly,

> The War on Terror, however, is not a real war. Its parameters are unclear, ranging from gunboat diplomacy to more or less gratuitous rights violations at home. Linguistic slippage threatens clarity of thought as the metaphor of war glosses over a great deal. Unlike the war against the Nazis, unlike even Vietnam, this war involves neither a fixed enemy nor an identifiable objective. There are no criteria by which to declare victory or recognize defeat. Closer to the War on Drugs than to 'hot' warfare as such, we find ourselves confronting an endless state of emergency that ensures the 'permanence of the temporary'. When the state intrudes on fundamental liberties, "temporary" tends to permanence as surely as night follows day.[62]

For the purposes of privacy protection, the most important difference between traditional warfare and counterterrorism is in the nature of the enemy. In traditional warfare the enemy is identifiable. Even in modern revolutionary asymmetric warfare, the ultimate goals of the insurgent will include establishing an alternative infrastructure and alternative governing structure. At that point in an insurgency, asymmetric tactics will take a back seat to the development of an alternative state structure, which can then be directly targeted by the threatened state entity.[63]

---

[61] See for example, Wayne McCormack, "Is it Crime or is it War? Toward an International Law of Terrorism", University of Utah S.J. Quinney College of Law Legal Studies Research Paper Series No. 05-01 online http://ssrn.com/abstracts= 747464

62 Wesley W. Pue, "The War on Teror: Constitutional Governance in a State of Permanent Warfare?" (Summer/Fall 2003) 41 Osgoode Hall Law Journal no 2/3 p. 267 at 269.

The War on Terror's distinguishing feature is that the politics of anti-Western Islamist terror are combined with radical theology to justify a long-term campaign of attacks with no real military elements, embracing instead an emotionally and theologically motivated series of attacks on largely civilian targets. It is the very nature of the West that inspires antipathy from elements within Islamic society, the West provides a visible alternative to fundamentalist life,

> More than ever before it is Western capitalism and democracy that provide an authentic and attractive alternative to traditional ways of thought and life. Fundamentalist leaders are not mistaken in seeing in Western civilization the greatest challenge to the way of life they wish to retain or restore for their people.[64]

By attacking the West, the relative power of the West to project its way of life into the Arab world might be reduced. There is as yet no effort on the part of the 'other side' of the War on Terror to create an alternative American or British or Spanish or Canadian government as would be expected under classical insurgent doctrine,[65] but instead an attempt to demonstrate the weakness of those powers' ability to protect their citizens and thereby cause those citizens to force governments to change their policies regarding various areas such as the Middle East. This eliminates the period of counterinsurgency warfare in which the transition is made from hit-and-run attacks to more traditional military operations, where a traditional state military can be most effective, and further delays or eliminates the potential for an "end" to conflict. Instead, a perpetual shadowy enemy exists, which cannot be targeted traditionally, but must be searched out both inside and outside a state's national borders. In particular, a terrorist cell within a state has, as one of its goals, to be indistinguishable on the surface from any other citizen. For this reason, it becomes possible to justify unprecedented observation of citizens by the state.

---

[63] United States Army Field Manual FMI 3-07.22 Paragraph 1-30.

[64] Bernard Lewis, "The Roots of Muslim Rage: Why so Many Muslims Deeply Resent the West, and Why Their Bitterness Will Not Be Easily Mollified", The Atlantic, September (1990) v. 266 n 3 p 47, at 53.

[65] United States Army Field Manual FMI 3-07.22 Paragraph 1-3.

A major byproduct of this strategy of non-warfare is an absence of recognizable enemies against whom to conduct combat. After the invasion of Afghanistan, and the toppling of the Taliban government there, one of the few governments in the world which was openly providing haven to Islamist terrorists such as Osama Bin Laden, there remained little for the collective military might of the West to attack. The invasion of Iraq, touted at the time as a vital step to prevent the use of CBRN weaponry by terrorist organizations, seems now at best to have transformed into part of a grand strategy to promote democracy as a method of ensuring stability of the current international system,[66] (a strategy which appears not to be effective, due to the difficulties of imposing a democratic form of government externally) at worst an ill thought out and pointless exercise in militaristic opportunism. It may well be argued, as it has by Bernard Lewis, that there is a fundamental cultural divide which makes the promotion of liberal democracy especially difficult in the Islamic world, for example "There is no word in Arabic, Persian or Turkish for 'Citizen'…. The word is absent in Arabic and the other languages because the idea – of the citizen as participant, of citizenship as participation – is not there."[67] Because of the necessarily drawn-out nature of the promotion of democracy in this way, this set of engagements has left the United States military and those of allied nations overextended in a way which brings into question the advisability of engaging in such adventures in the future.

---

[66] See, for example, Andrea Locatelli, "Towards Freedom and Democracy. Is Democracy Promotion a Viable Grand Strategy?" (2005) 5 Crossroads no. 1 pp. 5-12.

As military options are limited by the nature of the targets available, and traditional militaries are largely unable to engage in unconventional warfare of the type required to win a terrorist conflict, the first step along a long road towards what many perceive as victory is the identification of individuals within our own societies and around the world who are liable to engage in terrorist acts or to support terrorist organizations and to monitor and censure such individuals. In order to do this, we must first determine what terrorist groups are to be targeted by the War on Terror. Is it only a war on Islamist terror conducted by al Qaeda and its associated groups, or does the War on Terror include a general assault upon violent political groups around the world? The Canadian solution of providing a list of terrorist organizations proscribed by order in council seems to establish a defined "other" against which to struggle,[68] but while the official position may be that those are the groups to which we are opposed, the question remains: against which entities we will take any action? Are we censuring only active terrorists? Active supporters of terrorists? Or do we seek to target those who might fall only into the most technical definition of terrorism support such as those who inadvertently contribute to charities which fund terror groups?[69]

The next step, after determining the scope of how we define our enemy is to seek out the individuals who make up organizations which have been proscribed, and those outside those organizations who pursue similar goals by similar means. Since the makeup of modern terrorist groups is largely based upon political and religious attributes, one

---

67 Bernard Lewis, "Islam and Liberal Democracy: A Historical Overview" (1996) Journal of Democracy 7.2 52 at 54.

68 Commentary on the constitutionality of the particular measure of outlawing membership in an organization listed by order in council is a substantial matter in its own right and is outside the scope of this paper.

69 Nina J. Crimm, "Muslim-Americans' Charitable Giving Dilemma: What About a Centralized Terror-Free Donor Advised Fund?" (2008) 13 Roger Williams Law Review, Symposium Issue, Islamic Law ad Law of

obvious method to use in the search for terrorists is to seek to monitor individuals who ascribe to certain political and religious philosophies, and take an active part in those communities. For example, we can monitor the membership of Tamil expatriate groups, as these groups have been linked to suicide bombings in Sri Lanka, or we could investigate any Muslim man who has been to Afghanistan for more than a few days during the time that it was used as a location for terrorist training by al Qaeda. These approaches provide a flood of suspects, which must be examined by an already overstretched counter-terrorism apparatus, wasting resources and tying our security policy to ethnic and religious discrimination, which might result in a constitutional challenge.[70]

Without more substantive criteria regarding who might be likely to be a terrorist, the next obvious and easy choice is to monitor individuals based on the persons with whom they have contact.[71] In the United States, this process of attempting to use personal connections to find terrorists has resulted in the collection and data mining of billions of telephone records by the NSA.[72] This process has been criticized as an invasion of the privacy of millions of Americans, as, "Billions of call records were handed over and still are streaming into the NSA's supercomputers from AT&T Corp., BellSouth Corp., and Verizon Communications Inc."[73] Further, it has led to lawsuits against the companies involved for privacy invasion.[74] It is unknown what criteria are being used to search these

---

the Muslim World Research Paper Series at New York Law School no. 08-29 at 5.

70 David M. Tanovich, "Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention", (Summer 2002) 40 Osgoode Hall Law Journal no. 2145at 165

[71] See for example the case of Maher Arar and the subsequent inquiry into his rendition and torture at Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, online http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/index.html

[72] Paul Koring, "Tracking of calls sparks furor in U.S.: Phone companies gave data to NSA," Globe and Mail May 12, 2006, online www.globeandmail.com.

[73] Paul Koring, "CIA Nominee defends phone-data mining" Globe and Mail, May 15, 2006. online: globeandmail.com.

[74] Peter Grier, "For telecoms, a storm of lawsuits awaits." May 24, 2006 Christian Science Monitor. Online:

data records, or what other countries might be using similar techniques to investigate and control their citizenry. The program was authorized by President Bush in secret, and conducted over the course of years without public knowledge, without input from the legislative or judicial branches of government in the United States. Yet, "Two out of three Americans apparently agree that the hunt for al-Qaeda justifies the data mining of their telephone records and the no-longer secret program isn't a worrisome invasion of privacy…"[75]

Citizens who see terrorist attacks broadcast live on television are liable to experience a fear, justifiable or not, that they may be the next targets. The call for enhanced security is not only from a group of law-enforcement and intelligence special interests, it is from a majority of concerned citizens. The vast majority of people would never be sanctioned by any sort of counter-terrorist measures adopted by the government no matter how harsh and overreaching. Most people have nothing to hide from the government regarding terrorism, even among communities which would be likely to be subject to enhanced observation such as conservative Muslim groups. There is a likelihood, however, that any individual will be subject to scrutiny under this type of program. While most individuals do not have terrorist connections, it is possible to be in contact with suspected terrorists on a daily basis without one's knowledge, by definition, terrorists operate in secret. Once one is caught up in the counter-terrorist system, it becomes extremely difficult to become disentangled due to the lack of transparency in the system, and in some cases lack of due process. The danger of being subject to extraordinary rendition and held prisoner at some "black site" is a terrible one. It is partly because of the

---

csmonitor.com.

[75] Paul Koring, "CIA Nominee defends phone-data mining" Globe and Mail, May 15, 2006. online:

dangers posed by the counter terrorism system to those who are wrongly entangled that we need to keep a close watch on the manner in which our privacy is protected, but more importantly, it is to protect ourselves from perpetual observation and depersonalization that we ought to prevent the sort of technological surveillance state which is being put in place inch by inch in our society.

---

globeandmail.com.

2.3 What can Canada do to deal with terrorism?

Any increase in group or state security comes as a trade off with individual security, privacy, and monetary expense. The question which must be asked regarding how we deal with this trade off is to what extent we are willing to sacrifice these other areas for protection from terrorist attacks. We may never know in a concrete fashion the benefits gained from increased security within Canada, because a truly successful campaign against terrorism would mean that the scale of potential damage could never be known. While a plot might be uncovered before any attack takes place, we could never know if the attack would have, in fact, eventually occurred, how successful it might have been, and whether it would have come to light notwithstanding the enhanced security measures taken. It is therefore difficult to determine where it is appropriate to draw a pragmatic balance between security and freedom from government observation and interference because neither the potential for future damage nor the effectiveness of measures taken can be measured.

If no pragmatic balancing is truly possible in the context of trading off civil liberties with increased anti-terrorist security, we must then seek to adhere to principle in our assessment of how we will deal with this balancing. We as democratic citizens must ask what additional, incremental enhancement in our security is gained by sacrificing our civil liberties, and whether the damage which is thereby done to our society is justifiable in this context. We must also ask whether any increase in security is worth fundamentally changing our relationship with governmental authority. These questions are not ones which we can ask once and then ignore, but rather are ones which we must ask ourselves constantly, as our understanding of the world around us changes. The Canadian Anti-Terrorism Act was drafted in an atmosphere charged with fear and doubt regarding the nature and scope of the threat of international terrorism to Canadians.[76] Canadians, along with many others around the world, feared that global terrorism, particularly Islamist internationalist terrorism, was a monolithic force poised to commence a war on our societies on a scale and in a manner heretofore unseen. Canadians saw an ominous and distant alien culture whose unknown motivations and unknown uniformity of opinion and capacity for violence established it as a major perceived threat. We saw 9/11 as a harbinger of a new era of warfare between East and West, with Islam replacing the atheistic communists as the primary threat to our way of life. After several years, we can see that ignorance of our opponent has led to an over-estimation of the danger posed. There exists, certainly, an element within the international community that seeks to destroy Western society. This element is tiny and weak compared to not only the military, industrial, social, and ideological power of the West, but compared to non-extremist adherents to Islamic belief (for example, in the case of Islamist terrorism) or Sikhism (in the case of Sikh Nationalists) or any other non-extremist majority religious or ideological group. Just as much as our society needs to condemn terrorist action, we need to embrace the larger communities which form the basis for extremist offshoots. One certain way to alienate these moderates, however, is by treating them as suspects instead of allies. Take, for example the infiltration of Hindu temples in Canada and the United Kingdom by members of the Tamil Tigers, or LTTE;[77] if Tamil Hindus are marginalized through a campaign directed in a generalized way against temples operating in the West, alienation will likely result in disillusionment with government and potentially increased support for the LTTE.

---

[76] Kent Roach *September 11: Consequences for Canada*, (Montreal: McGill – Queen's University Press, 2003.) pp. 56-64.

[77] Human Rights Watch, "Funding the 'Final War': LTTE Intimidation and Extortion in the Tamil Diaspora", Human Rights Watch Volume 18, No. 1 (c) at 21

The same principle applies in ensuring that moderate elements in Islam are not driven away from engagement with the larger society.

Such a war between cultures has not materialized, and to the extent that sectarian conflict has arisen, it appears to have done so at least partly based upon the military actions taken by some Western powers including the United States in the aftermath of September 11. While terrorist attacks may well continue in the future, they will not pose so great a danger that we must drastically alter our societies to meet that danger. Indeed, the danger that we may face from heightened security and a focus on Muslim groups for scrutiny is an alienation of those groups, even those who are born and raised in Canada, leading to the potential for domestic terrorism, as in the case of the London Underground bombings[78] and abortive Toronto terrorist cell.[79]

We cannot allow ourselves the conceit of believing that we can attain perfect physical security, and we cannot ignore the fact that pursuit of perfect physical security, in addition to being doomed to failure, is also liable to drive more and more extreme invasions of privacy and personal security in the name of national security. Where government invasions of personal security overshadow the security threat to individuals from the terrorist attacks being combated, we must seriously examine our goals and how we wish to attain them.

---

[78] In July 2005, a number of bombs were set off on public transit in London England by terrorists who had been born and raised in the United Kingdom.

[79] A number of native-born Canadian Muslims were arrested and charged in relation to alleged plots to attack the Canadian Parliament.

3.1 The Definition and Relevance of Privacy in Canada

What do we mean when we use the term privacy, and what is its importance as compared with the importance of providing security from terrorist attacks on Canadians? Each student of privacy must ask, "If 'privacy' is such a universal human need, which gives rise to a fundamental human right, why does it take such disconcertingly diverse forms?"[80] For our purposes, it is not necessary to engage in in-depth analysis of the philosophical underpinnings of privacy, it is enough to define our terms and allow others to attend to the deconstruction. More important to us is the determination of what type of privacy ought to be protected as against the government. It is of little utility to argue the philosophical underpinnings of privacy at the expense of allowing genuine invasions of privacy to go unchecked. Privacy is what creates space for the development of individuals within society. Alysia Davies suggests three themes of privacy as being particularly relevant to the anti-terrorism context.

> The first is the freedom to explore various ideas, thoughts and/or belief systems without being compelled or assumed to commit to them. The second is the freedom from constant observation and monitoring, the "right to be left alone" identified by Warren and Brandies. The third is the freedom to choose whether or not to share intimate information and with whom.[81]

What is clear is that privacy, which is among the most intimate of human rights – to those who respect privacy as a human right – is largely contextual,

> Whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving

---

[80] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", (2004) 113Yale Law Journal , Yale Law School Public Law & Legal Theory Research Paper Series Research Paper # 64, at 1.

[81] Alysia Davies, "Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada", (2006) 3 University of Ottawa Law and Technology Journal, No 1, 249 at 263.

> information; their relationship to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.[82]

Different cultures conceive of privacy differently. In the Anglo-American tradition, there is a history of distrust of government stemming from the English and American experiences which influences the conceptions of privacy held by many in Canada. Canada also shares with the United States a frontier history and immigrant mindset which influences our thoughts on privacy. Immigrants and homesteaders are often people who are individualistic to a greater degree than others amongst the population, and they have a great influence on our culture. From our earliest history, immigrants to Canada have sought to free themselves from overbearing government, poverty, and crowded conditions by uprooting their entire lives and moving to a new place. These individuals tend to have a distinct sense of what is and is not the business of other people.

Generally recognized as one of the early defining works on privacy in the Anglo-American context was Warren and Brandeis[83] In this work, the right to privacy is likened to other non-property rights, and described as the right to be let alone,

> It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed... The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.[84]

---

[82] Helen Nissenbaum, "Privacy as Contextual Integrity", (2004) 79 Washington Law Review 119 at 155.

[83] *The Right to Privacy [The implicit made explicit]* Samuel D. Warren and Louis D. Brandeis, in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press, 1984) pp. 75-103

[84] *The Right to Privacy [The implicit made explicit]* Samuel D. Warren and Louis D. Brandeis, in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press, 1984)pp 82.

The right concerning Warren and Brandeis was mainly the right of privacy as against individuals and private interests, particularly the press, and to ensure that "the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity."[85] Privacy laws must take into account both public sector and non-public-sector invasions of privacy, although the remedies provided against either must, of necessity, be different. In the case of a public sector invasion of privacy, the victim is liable to have the weight of the government brought against him or her, which is difficult enough, but on the other hand, if one's private affairs are broadcast through the media, one is opened up to the inspection of society as a whole, and subject to the potential for humiliation and societal sanction, which, while lacking the legal authority of state sanctions, can be highly disruptive to one's life. Regardless of whether the invasion is public or private, "Some things all men alike are entitled to keep from popular curiosity, whether in public life or not, while others are only private because the persons concerned have not assumed a position which makes their doings legitimate matters of public investigation."[86]

We must recall in balancing security concerns with civil rights the nature of our society. Our tradition is one which respects and values the individual, and seeks to protect a secure society that is made up of individuals.[87] We do not lightly dispose of the rights of the individual in order to protect the state, we respect the individual's rights as the underpinning and central value of the state's existence. It is the case in our society that "The protection of society must come mainly through a recognition of the rights of the

---

[85] *The Right to Privacy [The implicit made explicit]* Samuel D. Warren and Louis D. Brandeis, in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press, 1984)pp 86.

[86] *The Right to Privacy [The implicit made explicit]* Samuel D. Warren and Louis D. Brandeis, in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press, 1984)88.

87 F.C. DeCoste, *On Coming to Law: An Introduction to Law in Liberal Societies*, (Markham: Butterworths,

individual."[88] To destroy or damage individual rights, then, is to damage our society as a whole, not to protect it.

The right to privacy, as defined in this early work, was concerned with publication mainly, rather than with the invasion itself. Personal information has become so much more valuable in the modern society that we must value privacy even in the absence of a publication of non-consensually collected data. This has led to the development of much modern privacy legislation and the idea of informed consent to the collection, disclosure and sharing of private information.

The importance of privacy has led to a legislative trend around the world wherein governments set out rules for the collection, protection, and dissemination of certain kinds of information by both government and private organizations.[89] These rules are generally directed towards information that is collected in the general course of events through disclosure by the individual whose privacy is in question. This covers a broad spectrum of information such as medical histories taken by health care providers, credit information collected in the course of business transactions, and personal information collected by the government in the course of collecting income taxes or census data. In all these cases, the subject is or should be aware that information has been collected, and why. In the case of surveillance and dataveillance, the subject is in no position to know that the data has either been collected or collated, by whom, why, when, or how. Obviously this is a much greater threat to individual privacy, as there is no baseline of knowledge on the part of the individual in question to allow them to monitor their privacy, yet proposals from the

---

2001) at 8-11

[88] *The Right to Privacy [The implicit made explicit]* Samuel D. Warren and Louis D. Brandeis, in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press, 1984) pp 90.

[89] See, for example, *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25.

Canadian Department of Justice would allow for a much looser treatment of such information.

3.2 Competing Conceptions of Privacy in the West

There are a number of competing conceptions of privacy in our culture, and competing conceptions of the importance of a right to privacy generally in the absence of consensus on the meaning of privacy. Privacy is often regarded as an important but vague notion, "In every corner of the Western world, writers proclaim 'privacy" as a supremely important human good, as a value somehow at the core of what makes life worth living."[90] Whitman, in trying to define privacy illustrates the fact that what is considered private depends largely on cultural context, however, there may be a tendency in this approach to draw too much from difference and not examine closely enough what different cultures have in common regarding privacy. While Whitman argues that European conceptions of privacy draw far more from the idea of personhood than American ideals which stem from the conception of liberty and inviolability of the home, he plays down the importance of similarities. Daniel Solove, on the other hand, attempts to draw together broad conceptions of privacy notions by drawing on a 'Family Resemblance' theory.[91] This approach may come closer to identifying key features of privacy by examining what differing privacy conceptions have in common, and establishing a broad and inclusive framework into which various notions can be fit.

> Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against.[92]

---

[90] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty", (2004) 113 Yale Law Journal, Yale Law School Public Law & Legal Theory Research Paper Series Research Paper # 64, Pg. 1 Online http://papers.ssrn.com/abstract=476041

[91] Daniel J. Solove, "Conceptualizing Privacy", (2002) 90 California Law Review 1087 at 1087

92 Daniel J. Solove, "'I've got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San

Rather than analyze the definition of privacy in general, more relevant in the context of Lawful Access is the question 'What type of privacy is it that we wish to protect as against our government?' It is unimportant to arrive at a consensus regarding the ideological or philosophical underpinnings of privacy if one's telephone conversations are being recorded or one's daily movements tracked. There are certainly areas where those who are generally philosophically opposed can agree that there is an area of privacy, that privacy in that area is important, and that invasions of that particular private area ought not to be countenanced. There is inevitably some degree of subjectivity in notions of privacy, simply because each individual may have differing conceptions of what is valued in terms of privacy because privacy is a feeling as much as a material fact.

"Privacy looks like a simple thing: it concerns the sensation we experience when we have the power to control information about ourselves and when we actualize that power in conformity with our interests, aspirations, and desires. Inevitably, therefore, there is a personal or subjective dimension to privacy."[93] Cultures view privacy differently. The American line of jurisprudence, for example, permits privacy only in matters not disclosed to third parties. This interpretation is long overdue for replacement in today's world of dissemination of information.[94]

There is often an air of paranoia in the discussion of privacy, "It is the rare privacy advocate who resists citing Orwell when describing [the dangers of invasion of privacy]."[95]

Diego Law Review, p. 745.

[93] Barry Cooper, "Privacy and Security in an Age of Terrorism", (October 2004) Fraser Institute Studies in Defence & Foreign Policy Number 3, at 8.

[94] Omer Tene, "What Google Knows: Privacy and Internet Search Engines" (2007) online at SSRN.com http://ssrn.com/abstract=1021490 at 71.

[95] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty", (2004) 113 Yale Law Journal, Yale Law School Public Law & Legal Theory Research Paper Series Research Paper # 64, Pg. 1

While Orwell may be mentioned, there is little reason to believe that current directions in privacy will lead to total observation of the individual to ensure loyalty to the state. The danger, however, is not in any one change in law leading to a police state, but rather in the creeping extension of observation by millimeters overturning the protections which have taken centuries to put in place. "Privacy is often destroyed by an aggregation of … minor encroachments, not always by a large exercise of state power."[96] It is vital to maintain a keen observation of the manner in which our identities and our privacy are protected from incursions in the name of providing total security.

We acknowledge that we will be seen by others as we move about on our daily business. We accept that our pharmacist might know about our health problems, we acknowledge that the government has a right to know, for the purpose of taxation, how much income we earn. Every day, we take part in interactions with others in which we exchange, amongst other things such as money or services, our privacy for goods, services, or social interactions. We accept these small but constant disclosures about ourselves because they do not tend to eliminate our general anonymity amongst the population, because we are aware of them and because they are more or less consensual. To the clerk at the video store, our selection of entertainment does not raise much interest or suspicion; to the bank teller, our chequings account is essentially uninteresting; to the gas station attendant, the fact that we have filled our tank more often than usual this week is neither here nor there. Because no individual has the capacity to draw together these disparate disclosures, no one can use these observations to develop an overarching view of an individual. A government which uses technology to agglomerate information about its

---

Online http://papers.ssrn.com/abstract=476041 citizens through data mining, has the resources to compile these individual disclosures into something more completely resembling a shadow of an individual's private life, and to track changes or patterns which may require closer scrutiny.

The vagaries of technology ought not to be the determining factor in how we deal with the interception of communications or acquisition of other private information. The determining factor in such issues ought to be principle, and that principle is the balancing of the need of individuals to communicate and live privately and the need of society to ensure its own security. Even as our physical security might be enhanced by intrusion into our communications, (and there is an excellent case to be made that this is simply not true to the extent that law enforcement officials would like us to believe, because of the technological problems associated with mass surveillance of communications) the security of our society as we know it is damaged by the diminution of our private sphere. It is as an association of individuals that our society is formed. We are not a collective, but distinct individuals all of us not only deserving but truly needing respect for our human agency in order for our society to function. The movement of government into our private spheres ought to be carefully balanced against the reason for doing so, with a mind to the importance of privacy to the well being of the individual and society.

---

[96] Daniel J. Solove, "Conceptualizing Privacy", (2002) 90 California Law Review 1087 1088-1155.

3.3 Why Privacy?

The fear of government intrusion into privacy is well rooted in, among other things, a reasonable suspicion of the activities, understanding, and motivations of public officials and bureaucrats. We do not implicitly trust people who do not know us and do not understand the context of our lives, at whose true motives, moreover, we can only speculate. Too often common sense and decency play only a small role in the day to day functioning of government. Where the demands of bureaucracy and an absence of personal moral responsibility make an unjust outcome easier or safer for an individual in an office of authority, there is a strong chance that decency and common sense will lose out. Even in cases where moral responsibility is taken by those in government, bureaucrats who expose abuse are ill protected from retaliation from those who pay the political price for amoral policy due to loose whistle blower protection. It is generally easier for a bureaucrat to abandon personal morality and common sense when applying policy rather than face the potentially unpleasant results of doing the right thing, whether that thing is exposing corruption and waste, or exposing the invasions of our privacy, or preventing the extrajudicial rendition of persons to states willing to practice torture.

> The exercise of public power is to be liberated from certain constraints by the imposition of others, which are primarily personal. Because the office is supposedly shielded from the personal interests of the one who fills it, what he does in his official capacity seems also to be depersonalized. This nourishes the illusion that personal morality does not apply to it with any force, and that it cannot be strictly assigned to his moral account. The office he occupies gets between him and his depersonalized acts.[97]

---

[97] Thomas Nagel "Ruthlessness in Public Life" In *Public And Private Morality* Stuart Hampshire ed, (Cambridge: Cambridge University Press, 1977) at 77.

As suggested above, too often in official life, acts which would defy common sense and personal morality are committed in the name of security or political expediency. Take for example, assisting in the extrajudicial deportation of one's own citizen to face torture in a third country at the request of an allied nation, based on a mere suspicion of association with terrorists in the case of Maher Arar. In that case, Mr. Arar received little help from the Canadian government as he was detained by the United States government and deported to Syria, where he was tortured.[98] Likewise we see that people who would normally never consider mass violations of human rights legitimate, when faced with an external threat, can rapidly go to extremes on behalf of a government, as in the case of the American administration's use of what has been come to be called the American Gulag Archipelago, mainly in Cuba and Afghanistan but also allegedly in other countries around the world. From the common gaolers involved in this program, to the pilots of the aircraft which whisk prisoners around the world under US custody, to the heads of the American Administration, there are likely few individuals involved who would, in their personal and private lives, seem any different from a typical citizen of the West. Their positions as part of the security apparatus, however, have created a sense that they are not only able, but obliged to engage in certain activities for the common good, which many feel violate the values of the Western democratic tradition. Happily, as time passes and the events of September 11 are seen more and more as isolated in their magnitude, rationality and control is returning to government in the West.[99]

---

[98] Online, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/index.html

[99] Seth F. Kreimer, "Rays of Sunlight in a Shadow 'War': FOIA, the Abuses of Anti-Terrorism, and the Strategy of Transparency", (2007) 11:4 Lewis & Clark Law Review 1141 at 1220.

The likelihood of policy exceeding the call of morality is even greater in the case of the context of the War on Terrorism than in ordinary government. Nagel's examples are drawn from the American involvement throughout Indochina during the Vietnam War and come from a context with a large, known, fixed enemy-the Soviet Union- which, although engaged in a struggle for international domination, followed certain rules in pursuing its goals.[100] Terrorism creates, psychologically if not actually, a similar struggle between fundamentally opposed cultures, but in this struggle, one side does not obey conventional rules regarding conduct, is not fixed, and is not subject to nuclear deterrence to stave off the worst excesses of behaviour. As a result, there is a fundamental shift in the methodology being used in order to deal with this threat as opposed to the threats posed by historically opposed nation-states. The new context creates even more motive for individuals to use their official functions as a moral screen to protect their personhood from terrible acts done in the name of the common good, this context encourages officials to engage in a 'race to the bottom' with terrorist organizations in a countervailing war of methodology. If extrajudicial rendition, torture, illegal spying and flouting the rules of warfare are the methods used by the 'good guys' how can we continue to identify them as such, except out of a fear of the potential for even worse conduct from opposed groups. How far will we accept this 'race to the bottom' to be run in our name?

The cost to the state of failing to detect terrorism would seem to outweigh personal qualms on the part of public servants regarding the justice of their actions. In order to prevent acts of terrorism, those persons in a position of authority may be inclined to overreach their authority, morality, or even common sense as a prophylactic response to terror, in which case, the human element which might normally act as a curb on the behaviour of state entities would be rendered ineffective. Horrified as they are by the methods used against the West, our officials may tend to see a need to respond in kind or with even greater severity to terrorist threats. The implications to a public servant of inaction on his or her part resulting in the facilitation of a terrorist act could also lead to overzealousness in the application of anti-terrorism laws dissimilar to that in, for example, ordinary criminal detection and enforcement. There are a number of reasons for this.

---

[100] Thomas Nagel "Ruthlessness in Public Life" In *Public And Private Morality* Stuart Hampshire ed, (Cambridge: Cambridge University Press, 1977) at 77.

First, any problem created by terrorism is an emergent problem, that is to say that the difficulties posed by terrorism are time sensitive. Whereas an organized crime network might be expected to operate in certain areas and certain ways consistently with a view to short and long term profits, a terrorist organization relies on surprise and asymmetric tactics, and as a result, if they are not stopped from conducting an attack at the first instance, there is every likelihood of mass casualties and the ensuing panic and physical and psychological disruption that follow. If they are detected but not captured or killed, terrorist tactics are liable to change and intelligence gathered in that regard to that point becomes less useful. There is therefore an incentive to take matters as far and as fast as they can be taken, even if that means that the rules and restrictions which might accompany a criminal investigation, or even military operation, must be abandoned.

Second, terrorism presents situations where many lives might be lost by acting slowly and methodically rather than taking effective action immediately and dealing with the consequences afterwards. The violent methods utilized by modern terrorists, such as suicide bombings, are able to kill many people in a single attack. Many thousands or hundreds of thousands might be killed if these terrorists are able to gain access to CBRN[101] weaponry. When this potentiality is measured against the value of privacy, the act of tracing e-mail or cell phone traffic or monitoring public areas with closed circuit television might seem innocuous. Indeed, isolated incidents of privacy invasion which result in successful counterterrorism operations would be perceived as highly beneficial. The difficulty here, however, is that the privacy invasions needed are not isolated, but massive.

Third, the War on Terrorism is perceived by many around the world as a clash of civilizations between the evangelical Christian fundamentalist movement allied uncomfortably with the Western secular tradition, which derives from the European enlightenment tradition, and fundamentalists within the Islamic world.[102] This clash is worthy of recognition, because whether it is acknowledged or not, it is acting on the minds of those involved. There is a clear 'Us' and a clear 'Them' in this current conflict, and for all the talk on the part of politicians of respect for other cultures and the non-representative nature of Islamist extremism, two fundamentalist religious groups are squared off for this continuing battle, and the moderate elements on either side are being dragged along with greater or lesser degrees of willingness. This clash is depicted by many on either side as a fight to the death between civilizations, or even an apocalyptic struggle leading to the end of the world. In such a clash, to allow personal feelings to override the needs of the day is less than likely for those who hold such strong beliefs.

All these factors establish an environment combining the impersonal and pervasive nature of technology with enhanced willingness to err on the side of security rather than on the side of individual liberty, where an individual might be subjected to arbitrary detention,

---

[101] Chemical, Biological, Radiological, Nuclear.

102 Gilles Kepel, *The War for Muslim Minds: Islam and the West*, (Cambridge: The Belknap Press of the

deportation, or even face torture based on probabilities and possibilities rather than clear evidence. Where such actions are possible, a desire to exclude government from one's personal affairs is not irrational, it is not paranoid, indeed it would appear to be virtually indispensable to persons concerned with their own safety and freedom. We need protection from our government because the power wielded by government combined with the tendency of individuals in official positions to place the ends of government ahead of private morality creates a potentially devastating mixture.

It is not only a threat of government sanction which causes us to desire privacy. As we have seen, it is against the prying eyes of other individuals, companies, the media and in fact anyone to whom we do not open our private lives against whom we seek to maintain privacy. The argument, "if private information is recorded and observed but no adverse consequences result, has there been an invasion of privacy?"[103] is not acceptable any more so in the case of the private sector than the public sector. Privacy is not simply the absence of sanction resulting from observation, it is freedom from observation itself. The damage done is damage caused by the invasion itself and a consequent reduction in the individual's feeling of security and personal well-being. Like a physical trespass, the damage in an invasion of privacy arises with a trampling of the (psychological) grass. Whether observed by government or industry or the next door neighbor, invasion of privacy is an affront to the freedom of the individual to be an individual, not forced to conform to an undifferentiated mass of humanity, and the right of that individual to be left to his or her own devices so long as he or she does not interfere with the well being of others.

University of Harvard Press, 2004) at 1-9.

[103] Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and Policies for Counter Terrorism* Robert Popp & John Yen, Eds. (Hoboken: IEEE Press, 2005) P 10.

3.4 Section 8 and Constitutional Protections of Privacy:

Section 8 of the Charter of Rights and Freedoms has been interpreted to include protection for privacy rights.[104] [105] This section states that, "Everyone has the right to be secure against unreasonable search or seizure." The criteria which have been established for examining the constitutionality of legislation under Section 8 are that:

1) There must be an expectation of privacy.
2) The expectation must be reasonable.

With regard to the first requirement, in respect of the areas covered by Lawful Access proposals, not only is there an expectation of privacy on the part of individuals in relation to tracking and transmission data, but that the expectation is reasonable. Different aspects of electronic data, whether content, transmission routing information, or information about subscribers to electronic services will attract differing levels of privacy protection,[106] but they must all have some degree of protection. To summarize the above submissions, the volume of information which modern technology makes available to investigators armed with the latest technology is massive and growing. Transmission data can reveal the entire social network of an individual, the degrees of contact, and details of one's personal life such as when one is awake and asleep, where one is at any given time, with whom one communicates, what one reads on the Internet, how often, and for how long. Tracking data, even more so, reveals intimate details about an individual, following movements with shocking precision through electronic means, and giving away an individual's travel and spending habits. It is not unreasonable for an individual to expect that their movements and communications be, for the most part and without very good reason, private from the authorities. The court in Canada has recognized core privacy rights:

---

[104] *Canadian Charter of Rights and Freedoms* Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.).

105 *Hunter et al.* v *Southam Inc.*, [1984] 2 S.C.R. 1421.
106 Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age", (2008), 12 Canadian Criminal Law Review 115 at 116-117.

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[107]

The Supreme Court of Canada has declared that "Section 8 protects people and not places."[108] Therefore, privacy can be expected even in public places. Public anonymity is a valuable commodity in Canadian society. Canadians ought to expect that unless one engages in behaviour that merits investigation in public, that one will be free to go about one's business without undue attention from the authorities. That is one great difficulty with the proposed Lawful Access provisions: they seek to target individuals for inspection on reduced grounds of suspicion, rather than reasonable grounds to believe that a serious crime has been is being or will be committed. Reasonable suspicion is a much lower standard to which to rise than reasonable belief, and the basis of reasonable suspicion is the underpinning for expanded searches within Lawful Access in relation particularly to terrorism offences – offences which are defined in an extremely broad fashion at any rate, and which lack precision and focus.

The notion of basing an incursion upon Section 8 Charter rights on a 'reasonable suspicion' is not new. Reasonable suspicion has arisen in recent jurisprudence as an appropriate standard for certain minimal incursions upon rights in certain circumstances. In *R.* v. *Mann*,[109] the Supreme court examined the use of search incidental to 'investigative detention', which is a state of pre-arrest detention used by police where there does not exist the grounds yet for an arrest of an individual, but there is the belief that there may be some cause to make inquiries with that individual. The issue in question in that case was whether evidence found during a search of the suspect incidental to investigative detention ought to be excluded as having been obtained through an illegal search. The court ruled that there would be cause to search individuals upon investigative detention in some cases, but that this did not amount to a parallel of the general power to search upon arrest. The search must arise from a reasonable suspicion that the officer's safety or that of others is at risk. [110] This suspicion, "…cannot be justified on the bass of a vague or non-existent concern for safety, nor can the search be premised upon hunches or mere intuition."[111] There is a requirement in the case of reasonable suspicion for there to be some evidence which can be pointed to by the authority that there is cause for the particular means applied. A search of an individual upon investigative detention must be based on objective evidence, not mere suspicion. What results is a standard lesser than the standard normal for searches, but greater than mere hunch.

---

[107] *R.* v. *Plant*, [1993] 3 S.C.R. 281.

[108] *Hunter et al.* v *Southam Inc.*, [1984] 2 S.C.R. 1421.

The court goes on in more recent jurisprudence arising from the use of 'sniffer dogs' for the purposes of locating narcotics to expand on the standard applicable in an environment where there is a reduced expectation of privacy such as a bus terminal,[112] or a public school.[113] The court was divided on a number of issues, however it held that the infringement of the Section 8 right found in Kang-Brown could be justified based on a ground of reasonable suspicion, but held the authority to a high standard in defining reasonable suspicion, requiring that there be some connection with the individual being investigated, not simply investigating every individual in an area where some crime of some variety is suspected to be taking place. The court held that "A 'reasonable' suspicion means something more than a mere suspicion and something less than a belief based upon reasonable/and probable grounds."[114] In this case the evidence obtained by the dog sniff was excluded as the investigating officer had not shown that there was any evidence that would engage a reasonable suspicion in the accused upon the search being made.

---

[109] R. v. Mann [2004] 3 S.C.R. 59.
[110] R. v. Mann [2004] 3 S.C.R. 59. at para 40.
[111] R. v. Mann [2004] 3 S.C.R. 59. at para 40.
[112] *R.* v. *Kang-Brown*, 2008 SCC 18.

Likewise in *R.* v. *A.M.*, the court found that while authorities may use dog sniff searches based on a reasonable suspicion, there is no grounds for a search based on generalized suspicion.[115] Reasonable suspicion is not the basis for a fishing expedition, there is a requirement for objective evidence that would indicate that a search ought to be made. In the absence of such evidence, the search will be illegal. So while reasonable suspicion is a lower standard, the courts have allowed it to be applied in certain situations where there is a reduced expectation of privacy, or in cases where such a search is for the immediate and justifiable safety concern of the officer involved. The question remaining to be answered is whether such a standard ought to be applied through legislation where it affects areas without a reduced expectation of privacy and where the infringement of the section 8 right is not minimal.

---

[113] *R.* v. *A.M.* 2008 SCC 19.
[114] *R.* v. *Kang-Brown*, 2008 SCC 18. at para 75.
[115] *R.* v. *A.M.* 2008 SCC 19. at para 12-13.

The *Criminal Code* at s. 492.2 sets out a procedure for the application for a warrant to obtain 'number recorder' information based on a reasonable grounds to suspect basis.[116] Number recorder information is information that indicates the calls received to and from a particular telephone device. In essence, it is a warrant to trace every incoming and outgoing number to and from a phone. While the constitutionality of this provision has been challenged unsuccessfully,[117] the courts have focused on the fact that the number recorder is a device that discloses a minimal amount of personal information. Other courts, however, have held that the use of number recorder devices is unconstitutional, as they do not comply with the standards set out in *Hunter* v. *Southam*.[118] The definition of tracking data as proposed under Lawful Access provisions would cover a great deal more than mere telephone numbers and durations of calls. It is still suspect as to whether a grounds of reasonable suspicion could be applied to Lawful Access as proposed by the Department of Justice.

Accepting, then, that any particular individual would have an expectation of privacy in relation to the information covered by the definition of tracking and transmission data. In determining the reasonableness of an expectation of privacy,

> Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement...[119]

---

[116] *Criminal Code* R.S.C. 1985, c. C-46, s. 492.2 (1)
[117] *Cody* v. *R.* [2007] QCCA 1276.
[118] *R.* v. *Nguyen et al*, [2004] BCSC 76.
[119] *R.* v. *Plant*, [1993] 3 S.C.R. 281.

will need to be the guidelines we observe. In this case the nature of the information is a core of biographic information about the intimate details of an individual's life. It would be obtained from parties who have collected this information under express or implied agreements[120] to keep that information confidential. It will be collected through the use of secret ex parte applications the existence of which will never be disclosed to the person being investigated unless criminal charges are laid. The seriousness of the crimes to be investigated, enumerated by the Department of Justice[121] as being particularly terrorist offences, are undisputable, but the real threat posed by them to society is minimal. As argued earlier on the relevance of terrorism to Canada, and indeed the Western democracies, it is concluded that while terrorism may provide spectacular news footage, the actual threat to an industrialized or post-industrial society must be placed in context. Our reaction to terrorism has created more of a monster than ever existed before through both the process of validation of terrorism as a significant global force, and through violent over-reaction in Middle East policy, which leads to a greater radicalization of people and groups never before drawn to radical movements.[122]

What kind of protection must we give to transmission and tracking data? The contextual examination of a purported privacy right is important. We must examine the full situation regarding the matter claimed to be private, and the context of the information.

> A reasonable expectation of privacy is contextual. The expectation does not have to be of the highest form of privacy to trigger the protection of s. 8. For example, someone who rents a hotel room does not *own* the room, and

---

[120] As required by privacy legislation enacted throughout the country, both federally and provincially.
[121] Department of Justice Canada "Lawful Access: Legal Review Follow up consultations: Criminal Code Draft Proposals February-March 2005." http://www.cippic.ca/uploads/JC_CCAmend_2.pdf
[122] Take, for example, the radicalization of native-born Canadians and other Western citizens of Muslim heritage, who make up the so called "homegrown" terrorist problem. This problem stems not only from radicalizing external influences on young Muslims in the West, but from the perceived injustices stemming from a shadowy "War on Terror".

> very likely understands that hotel management has a master key. A reasonable understanding is that hotel staff will access the room, but for limited purposes. There is therefore a reasonable expectation of some privacy in the room, which can be enhances by the display of a sign requesting privacy.[123]

While data held on a public computer network may be accessible to many individuals and people, it is similar to the situation of the hotel room, or rented locker, whereby an individual has intentionally or inadvertently (through their use of the network) stored data within the system in a belief that there will attach to it a certain level of privacy. Although e-mail and other electronic transmissions and data may be held within the electronic archives of a third party such as an Internet service provider or telecommunications provider, or point-of-sale service company, they do not lose their level of implied and express privacy. Indeed, the systems of electronic banking and communications would likely collapse were it to be the case that privacy was not assured in the use of these services.

The extent of the protection under Section 8 hinges on whether an individual has a reasonable expectation of privacy in regard to the monitored private matter. What expectation of privacy is reasonable is debatable and will vary from context to context. For example, in the case of *R.* v. *Wise*,[124] which examined the legality of the surreptitious implantation of an electronic tracking device into a suspect's vehicle without a warrant, the majority held that an individual has a reduced expectation of privacy in regards to his behaviour in a motor vehicle because,

> Society then requires and expects protection from drunken drivers, speeding drivers and dangerous drivers. A

---

[123] *R.* v. *Buhay*, [2003] S.C.R. 631, para 22

[124] *R.* v. *Wise* [1992] 1 S.C.R. 527.

> reasonable level of surveillance of each and every motor vehicle is readily accepted, indeed is demanded, by society to obtain this protection… although there remains an expectation of privacy in automobile travel, it is markedly decreased relative to the expectation of privacy in one's home or office.[125]

In this case the majority of the court held that because we have a decreased expectation of privacy regarding our state of sobriety or competence while operating a motor vehicle, we have a generally decreased expectation of privacy in our automobile including the locations to which we drive. In dissent La Forest J. disputes this particular application of a diminished expectation of privacy, indicating that the diminished expectation in this area was in relation to the operation of a motor vehicle on a public highway, rather than in the movements one makes in a motor vehicle.[126] This would seem to be a more principled definition of the reduced expectation of privacy in a vehicle. because LaForest's explanation of a reduced expectation of privacy in a motor vehicle is narrower, but still allows for the societal goal of ensuring safety on the roads. The Supreme Court still adheres to the majority in Wise, however it would be preferable for the purposes of providing greater certainty prior to the use of technology for surveillance purposes for the court to, at the very least, provide a more detailed outline of guidelines as to how they will apply their interpretation of privacy rights to surveillance technology. While the state may have a legitimate interest in the manner in which dangerous devices such as automobiles are used, they do not have a legitimate interest in the ultimate destinations of every individual traveling inside. It is the destination or location which is disclosed by electronic monitoring, and not necessarily the manner in which the vehicle is operated. LaForest J. foresaw the development of increasingly powerful tools for monitoring individuals, devices which we now see within our society. In examining modern technology, his dissent is preferable to the decision of the majority, as it reflects more closely the state of our society, and the state of technology. As such, the diminished expectation of privacy ought not to apply to tracking devices, particularly to modern devices which are much more advanced than those used in the instant case, which many individuals carry unwittingly.

---

[125] *R.* v. *Wise* [1992] 1 S.C.R. 527 at 534

La Forest J. establishes the principled connection to other more controlled forms of monitoring, quoting *R.* v. *Durate*, "If the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance." [127] and stating, "This equally applies to monitoring our every movement."[128] It is upon principle such as this that judicial and legislative control over constantly-changing technology must be based, because principle does not change with technology. It is irresponsible for a court to base a decision on technology which is subject to rapid change, because that decision will guide the treatment of new technology, even where the new technology is much more powerful and invasive than the old. If an approach by the Supreme Court is based on the technology available at the time, it is more than likely that the result will be as obsolete as the technology even before the judgment is released. If the fledgling nature of a relatively non-advanced technology for monitoring is used as cause to grant carte blanche usage to law enforcement agencies, it is only a matter of time before technological innovation or creative usage by the agencies creates a situation where a previously adjudicated technology has transformed into something that is much more intrusive into the privacy of individuals. The courts, when setting limits on the use of technology must recognize that

---

[126] *R.* v. *Wise* [1992] 1 S.C.R. 527 at 561

[127] *R.* v. *Durate* [1990] 1 S.C.R. 30.

technological advancement is incredibly rapid, and a line must be drawn early with a view to controlling the outcome of the use of technology to prevent abuse of that technology as it advances. "…one of the difficulties in assessing emerging technologies used in crime-fighting is that the information they reveal may change or increase as the science behind them develops further."[129]

In order to control technology, a section 8 analysis must not be based upon the realities of the current technology, whether it is accurate (say in the case of a tracking device) to locate only a compass bearing to a subject, or to locate a specific position within kilometers, meters, or centimeters. It should be immaterial whether a device can transmit data infrequently or frequently, accurately or inaccurately. What should matter is whether the individual has a right to privacy in his or her movements. Some have argued that location data ought not to attract the same protection as the contents of communications,[130] but this understanding of the importance of location data is flawed. Privacy is at least as much about freedom of movement without observation as about freedom from eavesdropping

The tendency to favour an examination of existing technology has not decreased in recent years, despite the phenomenal growth in the capabilities of technological privacy invasion and the rapid rate of development. In *Tessling*, the Supreme Court examined the use of FLIR[131],

---

[128] *R.* v. *Wise*, [1992] 1 S.C.R. 527 at 559.

[129] Alysia Davies, "Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada", (2006) 3 University of Ottawa Law and Technology Journal, No 1, 249 at 271.

[130] Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age", (2008), 12 Canadian Criminal Law Review 115 at 159.

[131] Forward Looking Infra Red Sensors - Devices which use an infra-red camera mounted in an aircraft to "see" heat sources such as individual bodies, vehicles, and, in the relevant case, high intensity lighting for indoor marijuana cultivation.

> ...the reasonableness line has to be determined by looking at the information generated by *existing* FLIR technology, and then evaluating its impact on a reasonable privacy interest. If, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist.[132]

Again here the Supreme Court has missed an opportunity to base law on principle rather than on changeable technology. Where there could have been a test put in place to establish on what grounds FLIR use, or any intrusive technological system, for that matter, by police would constitute invasion of privacy, the court simply indicated the reasonableness of that technology as it stood at that moment in time, and gave no assistance to the court hearing that "different case". As a result, there is no predictability regarding the time or way in which any particular technology becomes constitutionally unacceptable for the purposes of invasion of privacy, even though the court appears to have indicated that at some point an increasingly intrusive technology would begin to violate the constitution. The only way to determine this matter with any finality is through litigation and an extended, untimely, and expensive appeals process. An opportunity was missed by the court to provide real guidance to investigators and courts regarding the principles on which Canadian privacy law will be based. The court, in the following paragraph, adopts technology-centric view of privacy law,

> I agree with Abella J.A. that the specter of the state placing our homes under technological surveillance raises extremely serious concerns. Where we differ, perhaps, is that in my view such technology must be evaluated according to its *present* capability. Whatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise. FLIR technology at this stage of its development is both non-intrusive in its

---

[132] *R.* v. *Tessling*, [2004] SCC 67 at para. 29

> operations and mundane in the data it is capable of producing. It is clear, to repeat, that at present no warrant could ever properly be granted solely on the basis of a FLIR image.[133]

What is necessary is not an investigation of the current capacity of a technology, what is necessary is the formation of judicial or legislative guidelines regarding what types of activities are private and will therefore require greater judicial oversight where authorities seek to observe those areas.

It is important not to neglect the fact that technological developments have changed the nature of modern tracking data and its relation to the majority decision in *R.* v. *Wise*[134] by multiplying many times the precision and invasiveness of monitoring technology. The majority in *Wise* stated,

> It must be remembered that the tracking device used in this case was unsophisticated and indeed simplistic. It did not provide a visual record of the movement or position of the vehicle. Nor was it able to pick up and record conversations in the vehicle. Rather, it was capable of giving only a very rough idea of the vehicle's location... The evidence in this case was that the device was used intermittently as a back-up for visual surveillance of the appellant's car beginning on July 17, 1987, particularly to attempt to locate the vehicle when visual surveillance failed. Since the device was not capable of pinpointing the vehicle with any degree of precision, physical surveillance was always required to fix its proximate position.[135]

This basis for this early case in the Supreme Court regarding electronic tracking ought not to guide our understanding of the topic of tracking data today. The crude "beeper" device used by the police in *Wise* bears no resemblance to the modern GPS enabled tracking devices possible today, nor did the capability for using the inbuilt GPS capacity of a car, palm-pilot, or cell phone to track an individual within inches at any time without any knowledge on the part of the suspect exist when this decision was made. In 1987, in order to trace a vehicle or a person's location electronically, a specific tracking device would have to be implanted on that vehicle or person. In less than twenty years, however, technology has evolved to a point where a person cannot realistically avoid having their movements electronically tracked while still taking advantage of the communication and other technological conveniences common in society.

---

[133] *R.* v. *Tessling*, [2004] SCC 67 at para 55.
[134] *R.* v. *Wise*, [1992] 1 S.C.R. 527 at 527

Technology has advanced to the point that it is within the power of a government, through the application of electronic surveillance, to virtually eliminate privacy from an individual's life without the knowledge of that individual There is, indeed, a reason for our limitation on a government's ability to invade privacy,

> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States* v. *White*, supra, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.[136]

---

[135] *R.* v. *Wise*, [1992] 1 S.C.R. 527 at 534-535.

The technology available now allows not only the recording of communications, but of the movements of an individual with frightening accuracy and invasiveness. The Supreme Court in *Wong* followed up the *Durate* decision, saying,

> I am firmly of the view that if a free and open society cannot brook the prospect that the agents of the state should, in the absence of judicial authorization, enjoy the right to record the words of whomever they choose, it is equally inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious video surveillance. George Orwell in his classic dystopian novel 1984 paints a grim picture of a society whose citizens had every reason to expect that their every movement was subject to electronic video surveillance. The contrast with the expectations of privacy in a free society such as our own could not be more striking. The notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society. There are, as *R.* v. *Dyment*, 1988 CanLII 10 (S.C.C.), [1988] 2 S.C.R. 417, at pp. 428-29, tells us, situations and places which invite special sensitivity to the need for human privacy. Moreover, as *Duarte* indicates, we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."[137]

Based on modern technology, it would be possible for the authorities to track, even retroactively, a given individual's location and activities without leaving a well-equipped office, simply tracking his cell phone calls and GPS location, credit and debit card transaction locations, automobile GPS, Blackberry, or other electronic devices. Instead of acting as a supplement to visual surveillance, electronic tracking threatens to become a

---

[136] *R.* v. *Durate*. [1990] 1 S.C.R. 30. 43-44.
[137] *R.* v. *Wong*, [1990] 3 S.C.R. 36. para 14.

predominant method for surveillance. Indeed, many suspicious activities can be engaged in by an individual in his or her home through the use of the Internet. The tracking device contemplated in *Wise* is a thing of the past, and rapidly advancing technology has created an environment where technology has the potential to essentially eliminate privacy through electronic means. Our society is already tracked, monitored, observed, recorded, analyzed and minutely examined by any number of organizations. By providing law enforcement with a tool such as Lawful Access combined with data mining, we could effectively remove the residuum to the right to privacy in our society. Surveillance law must be flexible to respond to constant changes in technology.[138] The appellate courts cannot react quickly enough to control how technology is used in investigation, and because of this, the courts ought to establish that whatever the technology, it is the type of information collected, not the manner in which it is collected that is important, thus allowing the public and the government to know what areas of private life are safe from warrantless investigation.

How then do we apply appropriate principles to modern electronic tracking data? As much as our society may have a legitimate interest in ensuring that motor vehicles are operated in a safe and responsible manner, how much more important to our communication infrastructure not be used as a roadway towards acts of mass political violence? Where the goal of monitoring the vehicle in *Wise* was to trace the movements of a suspected serial killer who was allegedly responsible for several deaths, how much more willing will we be to monitor the movements or communications of individuals suspected of planning or carrying out massive attacks on ourselves or our allies, where the casualties could number in the thousands? In times of threat against society, members of the society are liable to be willing to make tradeoffs between privacy and security which would not otherwise be acceptable. Likewise, when examining violations of the Charter, either from a S. 1 perspective or a S. 24 analysis, courts in a society threatened by terrorism may interpret violations of rights in a more security minded context than those not faced with imminent danger.

---

[138] Daniel J. Solove, "Reconstructing Electronic Surveillance Law,"(2004) 72 The George Washington Law Review 1701 at 1740.

3.5 Our Privacy Rights:

We, as citizens of a democratic rights-respecting state, have the right to carry on our lives without fear that our government or others are constantly watching our every move, unless there is a judicially approved and monitored reason for so doing. Indeed there is a growing international recognition of a fundamental human right to privacy throughout the Western world.[139] There is some dispute about the philosophical underpinning and content of a right to privacy, but many of the elements of the right are reasonably well established in codes of practice, national legislation and international agreements. Some such elements include rights of access to information retained by an organization about the individual, the right that the information be accurate and that incorrect information may be corrected, that the information be securely held, and that the information collected be only what is reasonably necessary.[140]

These constantly developing privacy norms and our own domestic privacy legislation[141] are in conflict, however, with the perceived need for security forces to monitor potential terrorists and for police to pursue sophisticated criminal networks. It is not reasonable to expect that criminals or terrorists have access to information regarding ongoing investigations into their activities, but what about the innocent people whose privacy is invaded through these investigations? Should a cloak of security-related secrecy be drawn permanently against inquiry by individuals regarding their privacy status? And if so, how could we possibly believe that a complaints-based system of oversight of privacy matters as is currently in place would be acceptable?

---

[139] See, for example, *Montreux Declaration*, issued at the 27th International Conference of Data Protection and Privacy Commissioners, September 16, 2005. Article 11.

[140] *Montreux Declaration*, issued at the 27th International Conference of Data Protection and Privacy Commissioners, September 16, 2005, article 17.

[141] See, for example, *Privacy* Act, R.S.C. 1985, c. P-21. and *Freedom of Information and*

4.1 The War on Terror, Reasonable Expectation of Privacy, and Constitutional Protection of Privacy in Canada:

Section one of the Canadian Charter of Rights and Freedoms provides that, "The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only t such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[142] There has been a great deal of jurisprudence interpreting this section, including the early leading Supreme Court of Canada case, *R.* v. *Oakes*.[143] In interpreting this section, the court placed strict limitation on the manner in which section 1 is to be applied. The test in Oakes sets out three considerations once a prima facie charter breach is found to exist, to determine whether a charter breach should fall within the protections of Section 1.

> First, the measures adopted must not be arbitrary, unfair or based on irrational considerations. In short they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question: *R.* v. *Big M Drug Mart Ltd.*, ... Third, there must be proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom and the objective which has been identified as of "sufficient importance".[144]

The court goes on to state that, "The more severe the deleterious effect of a measure, the more important the objective must be if the measure is to be reasonable and demonstrably

---

Protection of Privacy Act, R.S.A. 2000, c. F-25.

[142] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*(U.K.), 1982, c. 11. s. 1.

[143] *R.* v. *Oakes*, [1986] 1 S.C.R. 103.

[144] *R.* v. *Oakes*, [1986] 1 S.C.R. 103. para. 70.

justified in a free and democratic society."[145] The court later expanded on this test setting out,

> In many instances, the imposition of a measure will result in the fill, or nearly full, realization of the legislative objective. In these situations, the third step of the proportionality test calls for an examination of the balance that has been struck between the objective in question and the deleterious effects on constitutionally protected rights arising from the means that have been employed to achieve the objective. At other times, however, the measure at issue, while rationally connected to an important objective, will result in only the partial achievement of this object. In such cases, I believe that the third step of the second branch of the *Oakes* test requires both that the underlying objective of a measure and the salutary effects that actually result from its implementation be proportional to the deleterious effects the measure has on fundamental rights and freedoms. A legislative objective may be pressing and substantial, the means chosen may be rationally connected to that objective, and less rights-impairing alternatives may not be available. Nonetheless, even if the importance of the objective itself (when viewed in the abstract) outweighs the deleterious effects on protected rights, it is still possible that the actual salutary effects of the legislation will not be sufficient to justify these negative effects.[146]

Leaving aside the applications of awful access which apply to the interdiction of child pornography and organized crime, which are not the focus of this paper, and examining the purposes of Lawful Access relating to terrorism, this paper will use the interpretation given by the Supreme Court of Canada to the purpose of the Anti-Terrorism Act set out in *Re: Application under s. 83.28 of the Criminal Code*, stating that the purpose of the legislation was the prosecution and prevention of terrorism offences.[147] Likewise, in the case of the application of Lawful Access to terrorism offences, it will be assumed that the application of any Lawful Access provisions to terrorism offences will be or the purposes of the prosecution and prevention of terrorism offences.

---

[145] *R. v. Oakes*, [1986] 1 S.C.R. 103. Para 71.

[146] *Dagenais* v. *Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835 at 887-888.

[147] *Re: Application under s. 83.28 of the Criminal Code* [2004] 2 S.C.R. 248 at para 39.

In order to determine whether the prima facie violation of our rights through the invasion of our privacy is legal, we must determine whether this invasion is justifiable in a free and democratic society. The application of the *Oakes* test requires us to determine whether the salutary effects of the measure (Lawful Access applied to terrorism investigations) overcome the deleterious effects of the measure, and whether the prevention and prosecution of terrorism offences is a matter of sufficient importance to justify the measure.

We must therefore examine and attempt to strike a balance between these competing interests. We must determine what kind of threat terrorism presents to our society and the importance of counterterrorism, as well as understanding how imminent changes in surveillance technology will affect the privacy of individuals. To this we must add an analysis of the effectiveness of security measures that might be taken to enhance security. "It is often assumed that the security measure taken to address the threat is effective, and the only remaining question is whether the liberty interest is strong enough to curtail the security interest."[148] This is simply not true. The balancing of the security and the liberty interest must also investigate the effectiveness of the measure to be taken. In the following section, this paper will examine the relative importance of the protection of privacy interests and the prevention of terrorism offences.

---

[148] Daniel Solove, "Data Mining and the Security-Liberty Debate", (2007-2008) GWU Law School Public Law Research Paper No. 278, 74 University of Chicago Law Review, forthcoming 2008.

4.2 How important is counterterrorism in comparison to privacy?

International terrorism is not new. What is new is the scale of some recent attacks, and the fact that they have occurred within the borders of Western states. They are made all the more intimidating because we have no overt state-level threat to occupy our collective consciousness as we did during the Cold War. Mass communication has created an environment which empowers individuals through information and communication to a greater extent than has ever been possible before, whether for good or evil. The empowerment of small groups and individuals to communicate and spread their brand of thought and opinion does not necessarily pose a threat to a functioning state, but where mass communication combines with massive violence, small groups can seriously affect the morale of a nation or the globe. The promotion of violence through mass communication and the increase in deadliness possible through the use of modern technology does not represent a threat to the rule of law any more than traffic accidents or common street crime. They do not do more harm, and by far more people are killed each year in the West due to any number of other causes than by terrorism.[149] The threat of terrorism is more psychological than physical.

Terrorism has long been one of the early techniques used by those who sought to impose unpopular radical ideology on others, because it does not rely on persuasion, as does a democratic process, but rather relies upon fear and intimidation. Terrorism itself cannot destroy Western society, but it acts as a political and social 'force multiplier' allowing the ideals of a smaller group to be imposed directly or indirectly on a fearful population. Terrorism is the asymmetric parallel of the totalitarian police state. It relies on fear and intimidation to promote the ideas and rights of a particular group at the expense of others, without resort to informed discourse. Insurgent terrorism and totalitarianism are two sides of the same coin - one embraced by the weak, the other by the strong. It would be a terrible thing if, in our pursuit of security, we devolved into a reflection of our enemies. The threat of terrorism lies, therefore, not primarily without, but within. We have the power to protect or destroy the society which we distinguish from that promoted by radical terrorists, and that power shall be exercised through our response to terrorist activities conducted against us.

---

[149] For example, in 1997, cancer and heart disease each killed over 50,000 Canadians, combining to kill more than half of the 215,000 Canadians who died that year. Even Pneumonia and influenza killed over 8000 Canadians that year, more than the total number of Canadians killed by terrorism in all years combined. Canadian Statistics – *Selected Leading Causes of Death By Sex*, online: < http://www40.statcan.ca/l01/cst01/health36.htm>

At this time, the actual physical threat posed by terrorism is low. This is not to say that terrorism, left unchecked, will not develop into a more serious threat to society, especially where it may appeal to large groups of disadvantaged individuals who are susceptible to the influence of radical ideology. Communist revolutionary violence in the nineteenth century may not initially have presented a genuine threat to the established state system, but it grew in influence to the point where it became a contender for the ruling political ideology in the world throughout the twentieth century. Communist internationalist violence in the 1960s and 1970s, however, failed to lead to communist revolution in the West.

Islamist violence may prove to be similar, a dangerous force, and one which may or may not lead to widespread revolution, or it may result in a realignment of conflict within our society from east-west as it had been during the Cold War to Islamic and non-Islamic. If viewed as an insurgency, the militaristic aspect of Islamism is in its early stages. The United States military recognizes three stages of insurgency, which is in turn drawn from Maoist insurgent doctrine, "…insurgents are first on the strategic defensive (Phase I), move to stalemate (Phase II), and finally go over to the offensive (Phase III)." [150] While not a major threat to Western societies at this time, this particular movement, which seeks to overthrow the rule of law in secular states through violence, presents a threat for the future, yet the greater danger that we face is creeping tyranny destroying our society from within. External forces differ from internal forces greatly in the threats that they pose to our society. A terrorist group can threaten exactly one thing in relation to our society: random violent acts of a terrifying but statistically insignificant nature. The damage that can be done to our society from within far exceeds that damage which is possible through terrorism, both in seriousness and in extent, and the most dangerous part is that those who would do this damage from within would do so with the best of intentions, and most likely with the democratic support of the grateful nations of the West. By the time we have achieved perfect physical security from terrorism through the creation of a surveillance apparatus and the systematic destruction of foreign enemies and imprisonment of internal foes, we would not recognize the state which had been secured.

Even if the Islamist terrorist movement ultimately fades away into political social and military irrelevance, it will no doubt be eventually replaced by another group using violence to achieve an ideological end which cannot be achieved through peaceful political dialogue. The nature of modern technology and mass media allows for small groups or individuals to draw such attention to a cause through the use of violence that it is inevitable that these methods will be used repeatedly in pursuit of dubious ends. It is therefore incumbent upon societies which embrace the rule of law to have in place a flexible, just, and effective system for combating political violence at the sub-state level. This system must reflect our commitment to the elimination of political violence from our society and

---

150 United States Army Field Manual FMI 3-07.22 Paragraph 1-30.

societies around the world, our commitment to ensuring that our country does not become a source of support for political violence elsewhere in the world, and our commitment to ensuring that our principles of freedom and the rule of law are maintained even in the face of the threat or use of violence. We ought not to abandon long cherished principles of the relationship between government and society due to an external threat that is, at best, a mediocre danger to our society. Notwithstanding the actual threat posed, the perception of threat is great. This is because,

> The public debate on policy issues – particularly on complex issues or novel problems with unknown consequences – is often dominated by these information entrepreneurs, including activists and the media itself, who attempt to engender information cascaded to further their own particular agenda. 'An [information] cascade is a self-reinforcing process of collective belief formation by which an expressed perception triggers a chain reaction that gives the perception increasing plausibility through its rising availability in public discourse.' The result is often that relatively minor risks can be overblown causing a high level of social anxiety, the expenditure or misallocation of significant resources, and the imposition of costly regulation in situations where other risks, of greater magnitude, are ignored.[151]

To a greater extent than ever before, the technological means exist in the hands of governments to monitor the people inside and outside their borders. Through closed-circuit television monitoring, tracing and monitoring of telephone calls and electronic information transfers such as fax and electronic mail, and even the use of RFID tracing devices and GPS enabled communications devices for the tracking of individuals and the use of data mining to interpret all of that information, it is becoming possible to use technical means to completely invade the privacy and anonymity of an individual without

---

151 K.A. Tripale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy

their knowledge. It is also conceivable for us to envision situations in which such an invasion are entirely justifiable and desirable on the part of even the most liberal society. By tracing the movements and communications of known terrorists, entire networks of terrorist cells might be uncovered, monitored, and ultimately disrupted, potentially saving thousands of lives. While this capacity is invaluable for tracking terrorists and combating terrorism, the question remains to what extent will we accept the invasion of our privacy by governments in pursuit of security, and how can we use the valuable and powerful tools to assist in providing security without granting carte blanche to government to invade privacy? Will this technology be used to track known terrorists, or will the powerful tools in the hands of government be turned to a broader section of society through ethnic and religious profiling? While the tools available to the state are powerful, they are not unlimited, and "Whether used as the sole factor, or one factor among many, profiling allows race, religion, or ethnicity to play a determinative factor in investigative decisions."[152]

The danger from Islamist terror lies not with terrorist acts, however damaging they might be, but with the way in which they distract from dealing effectively with the global cultural rift they expose as their cause. This rift cannot be mended or managed through the application of security assets or military activities. Terrorism is the symptom of a greater problem, that of a failure on the part of democratic powers to use their power to promote physical and economic security and democracy in a thoughtful and meaningful way, and our acceptance of oppression of many people due to practical constraints- economic, political, cultural and physical. The West may not be solely responsible for economic and

---

and the Lessons of King Ludd", (2004-2005) Yale Journal of Law & Technology 125 at 135.

[152] Sujit Choudhry and Kent Roach, "Racial and Ethnic Profiling: Statutory Discretion, Constitutional

social injustice in the developing world, "…but the poverty of, say, Algeria or Nigeria also owes a great deal to economic mismanagement by local elites. The underdevelopment of the Arab world despite access to capital by the barrel-load, speaks volumes about the cultural (and religious) obstacles to development."[153] Terrorism prompts a reaction from the West that refocuses energy from peaceful pursuits to activities which alienate large parts of the global population. The reaction of the West has resulted in greater suspicion and dislike, and is liable to result in more terrorism, not less. Our collective anger in response to terrorist attacks has had the effect of blinding us to realities of how we could more effectively enhance our long-term security. Even official government policy statements in Canada reflect the preferability of a solution to terrorism that examine the roots of the problem rather than the symptom, Canada's Department of Foreign Affairs, in 2005, stated that "We believe the best weapon against terrorist recruitment is the promotion of accountable, democratic governments that respect human rights, allow for peaceful dissent and fulfill the aspirations of their people."[154] This belief is all to often not put into action.

There is one major exception to the notion that terrorism, or rather terrorist acts, in and of themselves are not a major threat to our society. The caveat must be that terrorism in the absence of CBRN[155] weaponry is not seriously dangerous in terms of a physical threat to our society. The use of CBRN weaponry moves terrorism from a minor threat to one of significance. Francis Fukuyama elaborates his theory of the end of history in the context of CBRN terrorism, saying,

---

Remedies, and Democratic Accountability", (Spring 2003) 41 Osgoode Hall Law Journal no. 1, 1 at 2.

[153] Christopher Bertram, "Afghanistan: A Just Intervention", (2002) 6 Imprints: A Journal of Analytical Socialism, No. 2.

[154] Department of Foreign Affairs, Canada's International Policy Statement: A Role of Pride and Influence in the World", 2005 at 12. online http://geo.international.gc.ca/cip-pic/ips/overview-en.aspx

> There are certainly no new non-democratic powers to challenge the United States... But a terrorist organization armed with weapons of mass destruction is a different matter: Although the organization may be a minor historical player, the technological capability it can potentially deploy is such that it must be taken seriously as a world-class threat. Indeed, such an organization poses graver challenges in certain ways than nuclear-armed superpowers, since the latter are for the most part deterrable and not into the business of committing national suicide.[156]

Numbers of people killed by terrorists compared with traffic accidents, smoking, hospital errors[157], and common diseases are tiny.[158] The threat posed by conventional terrorists cannot rise even to the level of a threat posed by a small state against the West. Furthermore, the threat posed by rogue states with weapons of mass destruction[159] is far greater in terms of the physical threat posed, although states may be susceptible to traditional strategic deterrence models, while terrorists are not. Neither our country, nor other Western countries, are liable to collapse or even lose significant international influence due to conventional terrorist attacks. Provided that sufficient efforts are made to ensure the security of CBRN weapons and precursors and the weaponization of otherwise harmless technology such as aircraft, there is little that terrorists can do that will create real and substantive damage to the capacity of democratic states to function. Protecting items

---

156 Francis Fukuyama, "Has History Restarted since September 11?", nineteenth Annual John Bonython Lecture, Thursday August 8, 2002, Online http://www.cis.org.au/events/jbl/jbl02.htm

157 Canadian Institute for Health Information, "Patient safety in Canada: An Update" August 14, 2007 online www.cihi.ca at 6.

[158] Canadian Statistics – *Selected Leading Causes of Death By Sex*, online: < http://www40.statcan.ca/l01/cst01/health36.htm> .

[159] For example, North Korea, with a handful of suspected Nuclear Weapons, India and Pakistan, who are confirmed to have nuclear weapons, and who have continuing conflict with one another, along with Pakistan's susceptibility to Islamist influence, Iran, which may be seeking to establish a nuclear capability as quickly as possible, and Israel, which likely has a nuclear capability and the willingness to use it in any number of possible self-defense scenarios.

such as aircraft and chemicals from weaponization allows for the monitoring of items, not individuals, expanding public safety while having no effect on individual privacy.

Domestically, the enhanced security measures taken to protect us from terrorism may well be worse than the problem they are trying to solve, especially if the rapidly advancing technology of surveillance and data processing outstrips the controls which have been put in place to protect privacy. If we relax rules regarding the collection of private information about individuals due to the perceived need to protect us from terrorism and organized crime, we will be left with a dangerously narrowed private sphere.

4.3 How does a perceived terrorist threat alter the willingness of a society to abandon liberties and alter a Section 1 analysis:

Crisis breeds poor policy, and in an atmosphere of 'bringing terrorists to justice' a skewed moral compass is a real possibility, threatening the foundation of our liberal democratic society and placing its values in at least temporary abeyance. One of the critical tests for a society is how it reacts in time of crisis."[160] Using the threat of terrorism as a justification for the extensive measures taken in the Anti-Terrorism Act and other anti-terrorism measures presents two problems. First, by overestimating the dangers presented to our society by terrorism, it creates a false emergency, and second by declaring a status-quo[161] to be an emergency, it creates a perpetual emergency. With reference to the first problem, in his Speech to the Senate Special Committee on the Anti-Terrorism Act on Monday February 21, 2005, Irwin Cotler used a level of rhetoric apparently designed to continue to excite a sense in the Canadian people that terrorism is a threat worthy of combating using whatever means necessary, saying, for example,

> …we are not dealing with your ordinary or domestic criminal, but with the transnational super-terrorist…we are dealing with Nuremberg crimes and Nuremberg criminals, with hostis humanis generic, the enemies of humankind.[162]

This is rhetoric designed to create a sense that international terrorism is some kind of monolithic force, assailing the very foundations of democracy, on a scale with that of Nazi Germany or the Soviet Bloc. This is hardly reflective of the actual existence of a handful of isolated extremists whose cellular organizational structure prevents any kind of singularly coordinated attack on the West, but instead limits it to infrequent, although sometimes atrocious, attacks without any overarching operational goals. Terrorists are in large measure not dangerous on the scale of Nazi Germany or similar threats because they have no effective way to achieve their strategic goals through the application of their tactics.

---

[160] Amos N. Guiora, "Legislative and Policy Responses to Terrorism", August 2005Case Researh Paper Series in Legal Studies, Working Paper 05-30, online at http://ssrn.com/abstrat=793344 at 9.

[161] The Status quo of terrorism existing somewhere in the international community and in some manner affecting Canada, a situation which has existed for as long as Canada has been any kind of player on the international scene, and will continue to be the situation for the foreseeable future.

[162] Speech by the hon. Irwin Cotler, Minister of Justice and Attorney General of Canada on the occasion of an appearance before the Special Committee of the Senate on the Anti-Terrorism Act, Monday, February 21, 2005 Online http://canada.justice.gc.ca/en/news/sp/2005/doc_31398.html

There are three levels of planning and organization required to carry off a successful war-fighting campaign. First is the tactical level, which concerns itself with the physical actions which one's forces must take in order to gain immediate, small scale physical success against an opponent. Al Qaeda has tactics: suicide bombing and terror against civilians, propaganda, and a handful of others. Second, there must be a strategic plan, which sets out the ultimate goal of a conflict and the conditions which must be achieved to attain that goal. Al Qaeda and other Islamist terrorists appear to have a strategic goal of overthrowing Middle Eastern governments and ultimately instituting a global Islamist state. The third area of planning and organization is called the operational level, which, simply put, is the connection between tactics and strategy. It is through operational planning that it is determined how one can use one's tactics in order to achieve one's strategic goals. The difficulty for terrorists is that by their very nature as a cellular organization without an organized command structure they are unable to apply their tactical methods into an operational plan to achieve their strategic goals. The very organizational structure which makes them so difficult to detect and attack prevents their ultimate victory. This has long been a difficulty faced by insurgent forces, and in successful national insurgencies, there has inevitably been a stage at which the parallel pseudo-government of the insurgents has attained a critical mass and established itself as an alternative state government, fighting the previous government's military through a final conventional stage of warfare. In some states Islamist insurgencies have succeeded in this. Of particular note is, of course, the takeover of Afghanistan by the Taliban after the Soviet withdrawal. The fact remains, however, that no insurgent force has ever overthrown a modern Western state on its own territory.

The threat posed by Nazi Germany was that of global domination by organized national warfare, and was a threat external to democratic states. The threat posed by international terrorism is a threat in reality posed by democracies themselves and their reactions to terrorism. The danger posed by terrorists is to individuals, but the threat posed to democracy is minimal if we take reasonable steps towards prevention in accordance with the laws which were already in place before September 11. In Principle 6 outlined in his speech[163], Cotler cites the Proportionality Principle, requiring a response to be proportionate to the threat posed, and the Contextual Principle, which requires that Charter rights and any limits imposed on them be considered in the context of the factual situation surrounding the rights. If these areas are examined dispassionately, it will be apparent that the threat of terrorism is not nearly so great as it has been initially made out to be. It is a minor threat to individuals, and hardly at all to society as a whole.

"It is often merely assumed without question that the security threat from terrorism is one of the gravest dangers we face in the modern world. The threat, however, has been severely overstated."[164] The actual threat posed by international terrorism, not the imagined threat of a super-terrorist, is small. Around the world, countries have been besieged by terrorism for decades and have not collapsed, or, in the case of those countries who embrace democratic principles, totally abandoned those principles. The ordinary terrorist with ordinary weapons has yet to topple a strong democracy, even over the course of decades,[165] and while it is important to fight terrorism, the ordinary methods of intelligence gathering and criminal investigation, combined with international cooperation against terrorism ought to make up our response. By abandoning rights in order to combat a negligible danger, we do greater damage through legislation than terrorism can do through bombs and guns.

---

[163] Speech by the hon. Irwin Cotler, Minister of Justice and Attorney General of Canada on the occasion of an appearance before the Special Committee of the Senate on the Anti-Terrorism Act, Monday, February 21, 2005 Online http://canada.justice.gc.ca/en/news/sp/2005/doc_31398.html.

164 Daniel Solove, "Data Mining and the Security-Liberty Debate", (2007-2008) GWU Law School Public Law Research Paper No. 278, 74 University of Chicago Law Review, forthcoming 2008.752.

External and internal threats to the state and the nation have been used in the past to justify massive rights violations by the Canadian Government, such as the internment of thousands of Japanese Canadians during the Second World War, and the arrest of over 500 Canadian citizens during the FLQ incident.[166] These violations in the name of security rarely seem like a good idea in retrospect, and can lead to national shame and remorse. Let us not allow the post-9/11 period to be one of those sources of shame. It is not the actual threat posed by the victims of rights abuses, however, which will make up our society's, and to a great extent the judiciary's, assessment of how to deal with these individuals. If it were, the presence of a few thousand Japanese shopkeepers and fishermen in British Columbia during the Second World War would not have caused alarm. Rather it is the perceived threat. The use of excessive rhetoric to overstate the danger posed to society by terrorism will lead to abuse in the future. We may well congratulate ourselves that we did not intern thousands of innocent Muslim, Arab, and South Asian Canadians immediately after September 11 (although a large number of detentions did occur in the United States[167]) but to do so would be to miss the point. Even if the provisions for preventative detention and arrest without warrant based on suspicion are never used, and no-one is ever sanctioned for non-compliance with an investigative hearing, we have established a structure designed to reduce freedom in order to provide a false sense of security and to create an appearance of action while not actually addressing the underlying problem. Not only have we abused rights by creating a system designed to reduce them, we have done so for no reasonable cause. This is not acceptable, even where there is technical charter compliance. Michael Ignatief argues that "Terrorist attack can justify abridgements of liberty only if suspensions of liberty do actually enhance security." [168] Although a good starting point, this is a fairly bare standard to set, and we must add to it that abridgements will only be justified if the increase in security is reasonably balanced with the reduction in liberty and civil rights.

---

[165] For example, Israel, The United Kingdom and Spain have suffered consistent terrorist attacks causing significant casualties throughout much of the postwar era, and have not abandoned liberal democratic principles. In fact, during the period of ETA separatist violence, Spain made the transition from the Fascist Franco regime to a democratic constitutional monarchy.

166 In late 1970, the activities of the Front de Liberation de Quebec, an armed group in the Canadian Province of Quebec culminated in the imposition of the War Measures Act by the Canadian Federal Government and the application of martial law.

A major problem with relying upon a 'War on Terrorism' to justify the abridgment of civil rights is the problem that such an open ended crisis is essentially a justification for the extension of emergency powers indefinitely. The argument is ultimately this – declaring War on Terrorism, as opposed to a particular terrorist group calls for the continuation of a constant war against a type of behaviour which has an obvious appeal for severely marginalized political groups. Terrorism is liable to continue to be a force in international society for as long as there are severely marginalized groups within the global community, and depending on how broadly terrorism is defined, and in Canada it is defined broadly indeed, it can encompass a vast array of activities. It is, in other words, an un-winnable war. Un-winnable because there is no fixed enemy and no condition which, once achieved, we can declare victory or even loss. The problem with using a state of emergency to justify a Section 1 analysis in the case of a War on Terror is that the emergency can never be over, it can only change from threat to threat and in intensity, and many have argued that security concerns ought to trump concerns for privacy.[169] One cannot 'win' a War on Terror any more than we can win a war on crime, or poverty, or illegal drugs. These things are products of human society, and cannot be eliminated. If we accept the proposition that rights should indeed be significantly different during times of emergency than in non-emergent situations, it falls to us to establish from the outset of the emergency what recognizable conditions will constitute the end of an emergency, and in this case that is not possible. While the inclusion of sunset and mandatory review provisions in the Anti-terrorism Act ensure that at the very least a debate will ensue, the initial justification of limitations on rights must be examined in the context of the perpetual nature of terrorism.

---

[167] American Civil Liberties Union, "Detention," (2003) online: American Civil Liberties Union http://www.aclu.org/safefree/resources/16828res20030707.html .

Any limitations on rights brought about to combat terrorism will be permanent unless they are struck down by the courts as unconstitutional or rescinded or replaced by Parliament for reasons of ineffectiveness, political gain, or principle. They will not be eliminated due to the end of terrorism. Scrutiny is demanded of our leadership where there are attempts to justify limitations of liberties due to apparent emergency, "There are two types of questions to ask about these emergency circumstances. First, are they actually necessary? And second, even if they are necessary, will they diminish respect for laws and rights in the future?"[170] The nature of the threat to democracy, or lack thereof, from terrorism does not establish an emergency, and reacting as though we were in a state of emergency will permanently diminish rights without a chance of restoring them. Even where such abridgements of rights are purportedly justified under a Section 1 analysis, "It is not healthy when criminal justice policy is defined by minimum standards that citizens can expect courts to impose on their governments."[171] It is the role of courts to act in protection of rights where legislative and executive branches overstep their bounds, and we as citizens must embrace and encourage this role,

---

[169] Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror*, (Toronto: Penguin Canada, 2004) p. 29.

> Courts should not be criticized for judging the effectiveness of anti-terrorism laws when those laws violate rights because the question of whether a measure is rationally connected to preventing terrorism and whether there are less rights invasive alternatives are central components of the proportionality analysis that is the foundation for modern rights protection. Courts can enrich the sources of anti-terrorism laws by imagining and describing less restrictive alternatives to current anti-terrorism measures.[172]

Let us take as an example the internment of Japanese Canadians during the Second World War. There was, indisputably, an emergency taking place during the course of the Second World War, a global war between two alliances of great and middle powers was in progress, and there was a very real fear amongst the public, if not a reality, that enemy agents might be lying in wait to spy, sabotage and kill. Unfortunately for the Japanese Canadians, they were easily identifiable to the general public and, unlike German and Italian immigrants, they belonged to a culture which was alien to the majority of Canadians

---

169 Kenneth Einar Himma, "Privacy vs. Security: Why Privacy is Not an Absolute Value or Right", online http://ssrn.com/abstract=994458, forthcoming in University of San Diego Law Review, at 13.

[170] Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror*, (Toronto: Penguin Canada, 2004) at p. 29.

[171] Kent Roach, *September 11: Consequences for Canada*, (Montreal: McGill – Queen's University Press, 2003.) at 76.

172 Kent Roach, "Sources and Trends in Post- 9/11 Anti-Terrorism Laws" (April 2006) University of

at the time. Germans and Italians, however different their culture may have been from the British and French Canadian majorities, came from a European Christian background that was familiar and comfortable. The Japanese were an alien group who looked different, often practiced different religions, and came from a divergent cultural background. They were obviously 'other' and, as such, were cause for fear amongst the majority. The threat perceived from Japanese Canadians was much like the threat perceived from Muslim Canadians after 9/11 – the potential for sleeper cells of seemingly harmless immigrants and native born citizens, secretly loyal to an alien power, and biding their time until they are ready to attack Canada from within. The major differences between the two situations were that there would be an identifiable end to the crisis of the Second World War in the immediate post-war period, whereas the War on Terror is potentially permanent, and the threat posed by the Axis powers was very substantial. The result of the treatment of Japanese internees, upheld at the time in the courts, was national shame and embarrassment, and a permanent stain on our nation in what is considered one of our darkest moments. Emergencies blind us to the damage that we do to ourselves in the name of security.

Lord Wright, writing on the issue of deportation of Japanese Canadians after the end of the Second World War succinctly illustrates the extent of deference by the Judiciary to the Executive in times of emergency,

> …if it be clear that an emergency has not arisen or no longer exists, there can be no justification for the exercise or continued exercise of the exceptional powers. The rule of law as to the distribution of powers between the Parliaments of the Dominion and the Parliaments of the Provinces comes into play. But very clear evidence that an emergency has not arisen or that the emergency no longer exists is required to

---

Toronto Legal Studies Series Research Paper No XX-06, at 28.

> justify the judiciary even though the question is one of *ultra vires*, in overruling the decision of the Parliament of the Dominion that exceptional measures were required or were still required. To this may be added as a corollary that it is not pertinent to the judiciary to consider the wisdom or the propriety of the particular policy which is embodied in the emergency legislation.[173]

Although the War Measure Act[174] and the National Emergency Transitional Powers Act[175] granting nearly unlimited emergency power to the executive branch of our government are no longer with us, emergencies can influence the constitutional interpretation of rights-offending statutes. What "…can be demonstrably justified in a free and democratic society,"[176] differs within the context in which that society exists. History has proved that in emergent situations, the courts have leaned towards protecting the society ahead of the individual.

---

[173] *Co-Operative Committee on Japanese Canadians et al.* v. *Attorney General of Canada et al.* [1947] 1 D.L.R. pp 585-586. (JCPC)

[174] *War Measures Act*, R.S.C. 1927, c 206.

[175] *National Emergency Transitional Powers Act*, S.C. 1945, c. 25.

[176] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*(U.K.), 1982, c. 11. s.1.

5.1 Dataveillance and Canadian Society: Tracking Data, the Electronic Age, and the Panopticon:

Through the increasing collection and interpretation of information via automated systems, and the potential for data mining to become a standard tool in law enforcement and intelligence organizations, we must examine the effect that these technological developments will have on our society, how communications technology, especially the Internet, is changing our society, and the utility of the Internet as a tool for privacy.

> Electronic surveillance presents additional problems. It is a sweeping form of investigatory power. It extends beyond a search, for it records behaviour, social interaction, and everything a person says and does. Rather than a targeted query for information, surveillance is often akin to casting a giant net, which can ensnare a significant amount of data beyond that which was originally sought. [177]

Because of the fundamentally different nature of electronic panoptic surveillance from traditional surveillance techniques, it requires particular consideration regarding how and why it will be used. The law surrounding dataveillance is in flux. Enforcement agencies are seeking to broaden their use of dataveillance, while the public has an interest in controlling its use. With the pace of technological change accelerating, the courts and legislature have an opportunity to tie privacy protection to the underlying privacy interest invaded rather than the technological means used to invade them.

---

[177] Daniel J. Solove, "Reconstructing Electronic Surveillance Law,"(2004) 72 The George Washington Law Review 1701 at 1707.

5.2 Is the Reaction against Dataveillance just Paranoia?

When Sir Robert Peel established the first modern police force, the London Metropolitan Police, there was an outcry that a government police agency was sure to become an instrument of terror in the hands of the executive branch of the government. While this was not the case in England, in many states that is precisely what the police have become. Throughout much of the Western world, however, based on the model of policing that was laid down in London, the safety and security of the public is greatly enhanced to the extent that it is impossible to imagine a modern Western society without an effective police force. Is the outcry against government intrusion into privacy and public anonymity simply more of the same? Do we rail against what is ultimately a public good, which inevitably will become as much a vital part of our society as a professional police force?

I suggest that the difference here is that while the establishment of the Metropolitan Police was done based on thoughtful principles which have become foundational to effective policing around the world, and showed the public the respect which they deserve, the invasion of privacy in the current context is being instituted in a purely expedient manner, showing deference more to the needs of the bureaucracy, the government, and law enforcement, than to the rights and needs of the public. Indeed while there is indisputable need for a modernization of how communications surveillance is overseen, the very need for enhanced investigative tools and lesser burdens of proof for warrants is questionable. Structures which violate the fundamental rights of citizens must not be established with an eye only to expedience and lip service to protecting rights. We must base organized incursions on rights on strict principles to which we recognize a duty to adhere, otherwise we are on the down side of the slippery slope upon which so many arguments about civil liberties centre, and we will have no rational basis upon which to determine how we will balance the needs of the many against the rights of the few or of the individual.

5.3 Interception of Electronic Mail and Monitoring of the Internet

The average person in Canada probably believes that his or her e-mail is more secure from prying eyes than it really is. The reality of e-mail is that it can be intercepted at a number of points in its transit from one user to another, whether by the local system administrators, the administrators of intervening systems, by criminals seeking private information or by authorities who may be engaged in the Internet version of a wiretap. Our behaviour regarding e-mail is guided by the idea that it is a reasonably private medium, like its physical analog, traditional post. A great deal of the utility of the e-mail system stems from its rapid and private nature. Much like traditional mail, we have come to rely on the fact that although it is technically possible to open and read mail at virtually any point in its transmission, this will not occur. The value of privacy in mail has been supported by laws surrounding interference with mail.[178]

> By erecting a legal structure to protect the privacy of letters, our society shaped the practice of letter writing and using the postal system. It occurred because of the desire to make privacy an integral part of these practices rather than to preserve the status quo.[179]

If we desire to maintain private interpersonal communication via written media into the technological age, we must embrace the idea that it is as invasive of privacy to intercept and read a person's e-mail as it is to intercept and read a person's physical mail. To argue that the fact that it is easy to illicitly read a user's mail makes it somehow more justifiable is nothing more than ridiculous. Both e-mail and its physical counterpart are manifestations of written communication between parties which is expected by both parties to be private. Both types of communication ought to be accorded the same level of respect.

---

[178] See, for example *Constitution of Mexico* (1917) Title I, Article 25. and *Postal Services Act,* (U.K.), 2000, c.26, s. 84. (see appendix C)

[179] Daniel J. Solove, "Conceptualizing Privacy", (2002) 90 California Law Review 1087 at 1142.at 1143

Likewise, the use of the Internet as a broad means to search out criminal activity ought not to overtake the social and economic usefulness of the medium.

> Proportionately, the social harm that will result if people's use of the Internet is impeded or chilled outweighs the social value that will be had in terms of the number of criminals who could be 'caught' by fishing on the Internet. Therefore, like a telephone wiretap, the primary use of Lawful Access should be as an extraordinary investigative technique as opposed to a facility for general surveillance. It seems reasonable to expect that an individual will be a suspect before the process is invoked to obtain Internet communications. This being the case, those seeking any kind of warrant under Lawful Access proposals should be able to achieve the higher threshold of proof (ie. reason to believe).[180]

The Internet represents one of the greatest advancements in communication and information technology in the history of mankind. The speed and ease with which people all over the world can communicate with one another and with which people can find information is far beyond that which has been possible before. The marketplace of ideas is expanded, just as the economic marketplace is expanded. It is now possible for virtually any business in the world with access to the Internet to sell to any other individual or business regardless of location. Through electronic matchmaking services, methods for the initiation of personal interaction between individuals have been profoundly changed. An increasing number of people are searching for and finding companionship through the Internet. All of these things are changing the way we live and interact with the world, and it is at this transitional time that we must recognize the importance of integrating our core values into the framework of human interaction represented by the Internet. The danger of decreased privacy is the evil twin of the expanded market of communication represented by the Internet. The threat to the public is clear,

---

[180] Letter from Office of the Information and Privacy Commissioner (Alberta) to Irwin Cotler April 11, 2005 Regarding Lawful Access Proposals. online: http://www.oipc.ab.ca/ims/client/upload/Lawful_Access_April_11_2005.pdf

> With the increasing use of such sophisticated technology, a great deal of personal information (eg. In the form of electronic mail, Internet and 'listserv' postings, cached information or data stored on computers) can be and is transmitted and distributed electronically. Technology is also making it easier to find, track, intercept and store such information and communications; this makes possible the compilation of more and more information about people, their habits, preferences and other information, the creation of larger and more detailed databases, and the ability to match the electronic data with other kinds of information – all much more quickly and to an extent wider than was previously possible in 'real space'. The decrease in the ability to guard one's privacy is thus both quantitative and qualitative.[181]

It is easy for individuals within a governmental organization to forget that society does not exist for the sake of governance, rather that governance exists to serve society. As such, the initial inclination of the authorities in regards to Internet security is to extend control as far as possible by, for example, requiring providers to build in means for the government to monitor communications, and reducing the evidentiary burden required to legally monitor the communications and activities of an individual. This will not assist the development of the electronic sector of the economy, rather it will instill suspicion in the user.

> Like the traditional storefront economy, the new web-based economy is dependent on establishing and maintaining trust. Routine government surveillance is as capable of

---

[181] Mary W.S. Wong, "Electronic Surveillance and Privacy in the United States After September 11, 2001: The USA PATRIOT Ac",(2002) Singapore Journal of Legal Studies 214 at 229-230.

> undermining that trust as poor corporate security. Nor yet is trust enhanced by transforming companies doing online business into virtual agents of the state. And yet, since 2002, federal legislation has been passed that encourages or even requires such entities to engage in surreptitious evidence gathering.[182]

Some have chosen to object to such invasions, for example librarians in the United States have objected to the release of information regarding the reading habits of their patrons.

> Last June, a library user who took out a book there, 'Bin Laden: The Man Who Declared War on America' noticed a handwritten note in the margin remarking that 'Hostility toward America is a religious duty and we hope to be rewarded by God,' And went to the Federal Bureau of Investigation. Agents, in turn, went to the library seeking names and information on anyone checking out the biography since 2001. The library's lawyers turned down the request, and agents went back with a subpoena… The library fought the subpoena, and the F.B.I. withdrew its demand.[183]

The surreptitious monitoring of individuals who might make such annotations (a quote from Bin Laden in a book about Bin Laden) and basing the outcomes of enforcement decisions on such monitoring is liable to be ineffective, is simply grasping at straws. How many millions of people have taken a keen interest in terrorism since September 11, 2001? How many hundreds of thousands have taken such an interest that their library records would place them in jeopardy of counterterrorism investigation on the basis of a suspicion of terrorist sympathies based on the above passage? Are investigative bodies so starved for leads that they are reduced to tracking such trivial minutiae? Yet the monitoring of library records is only a drop in the ocean of potential violation of personal privacy when compared with the monitoring of an individual's Internet activities.

---

[182] Letter from Office of the Information and Privacy Commissioner (Ontario) to Irwin Cotler April 21, 2005 Regarding Lawful Access Proposals. Online at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16087&N_ID=1&PT_ID=11457&U_ID=0Page 2 of 12.

[183] Eric Lichtblau, "Libraries Say Yes, Officials Do Quiz them About Users," New York Times, June 20, 2005. online: http://www.nytimes.com.

In a sense, monitoring of an individual's web surfing is much akin to monitoring of his or her library transactions. The Internet is a vast resource of information and knowledge as well as a tool for communications. The interconnected nature of it lends itself to progressive, lateral research methods which might lead an individual along a different trail of ideas than might otherwise be obvious. While this path might often be a dead end, it is often a convoluted path towards an interesting synthesis of ideas. The other side of this equation is that an individual might come across information which he or she might never have normally found, information that they might deem irrelevant, unnecessary, or even blatantly incorrect or offensive, such being the nature of the Internet, but they will likely view this information in the course of web surfing on a fairly regular basis. Monitoring patterns of Internet use will certainly not indicate with any ease whether or not an individual is liable to break the law. Rather it will show the innate curiosity of the individual.

An additional problem with monitoring Internet usage is a method of enhancing security is the sheer volume of material to be monitored. Without electronic data mining utilities, monitoring of the Internet would be so vast a task as to be unimaginable. Data mining is the key to modern surveillance. Without the prospect of electronic filter programs to sort through the hundreds of millions of web user's habits, the notion that Internet activity would be monitored would seem quaint or naïve. One imagines a building full of cubicles manned by tired civil servants searching for the criminal needle in a thousand haystacks of searches for cookie recipes and nude photos of celebrities. By adding the technology of today to the search, we find that an unthinking, untiring computer program would be invading the privacy of individuals and providing authorities with warnings based on arbitrary criteria. Make the search too specific, everything will fall through the cracks, make the search too general, and we return to the initial problem of too many pieces of information to examine and too few resources. Internet search engines agglomerate a massive amount of information about the stream of electronic thought in the world, and such information is ripe for data-mining.[184] Were data mining of Internet searches in Canada to be in place at this time, the research for this paper would be likely to come under scrutiny due to the nature of web searches performed in the preparation of this paper.[185] Monitoring Internet use is a combination of ineffectiveness and abuse of privacy and freedom of expression. While a total monitoring of the Internet would be impractical even for modern data mining computers, it would certainly be possible for an organization to designate subversive and dangerous web sites and monitor the traffic to those sites as a means of finding potential suspects in an investigation. This technique is, of course, used on a less technically advanced level by having undercover police officers monitoring and participating in Internet chat rooms known to be used for the proliferation of child pornography.

This technique is likely also used by intelligence and security services in the monitoring of Internet chat rooms relating to Islamist fundamentalism. When this particular technique is compared with the indiscriminate monitoring of mass use of certain web sites, it would appear to be less invasive and more focused, allowing the undercover

---

184 Omer Tene, "What Google Knows: Privacy and Internet Search Engines" 2007 online at http://ssrn.com/abstract=1021490 at 2-3.

[185] During the course of researching this paper I have examined such diverse and potentially subversive topics in more or less detail as Islamist fundamentalist doctrine and theology, details of airline and airport security, infrastructure security, techniques and methods for the production of homemade explosives and other terrorist techniques and devices and sub-national CBRN proliferation. An assortment of searches coming from one person which would almost certainly trigger some level of investigation were they to come to the attention of

officer to focus on activities that are actually criminal - the trading of child pornography - and taking place in a public forum. There can be no expectation of privacy in an Internet chat room, because one is communicating directly with whomever might be in that room without regard to who they might, in reality, be. Statements made in a chat room or on a forum or bulletin board are in the nature of public statements. They are not akin to private telephone calls or letter mail. The monitoring of public media on the Internet is certainly constitutionally valid as a means of monitoring criminal activity. The monitoring of transmission data of private communications and web-surfing is not. Of these, the monitoring of web surfing may well be the more important concern.

---

the authorities.

5.4 Electronic Tracking Data collection:

A less obvious but potentially even more invasive threat to privacy than the monitoring of web surfing and e-mail s the monitoring, on a reduced evidentiary basis, of tracking data. Even constant video monitoring of public places is far less invasive of privacy than dataveillance. While the public may have a more visceral reaction to being physically or remotely looked at through optical monitoring, "video cameras can provide real-time information on what people are doing within camera range, but do not provide information on who is doing it."[186] This statement may go too far, but it is true that in the case of CCTV, the activity is monitored separately from the individual, and a substantial effort is required to link an individual to an image, whereas dataveillance can be linked easily to individuals. Tracking data, on the other hand, covers virtually one's entire 'electronic signature.' It includes such things as where one uses one's ATM card or VISA, e-mail addresses they sent messages to, where their cell phone's GPS locator has been, and any number of other identifying pieces of information which, taken together, give a remarkably invasive picture of one's life.

> It is not necessary to 'listen in' *live* to electronic communications in order to capture an in depth data-rich composite of our private and personal activities, movements, intentions, relations, and associations. Access to data stored by telecommunications companies, ISP's, banks, other business and institutions, and at home can reveal that personal profile at any time of the day or night. Indeed, the private content of our *live* telephone communications may be dwarfed by the private content in the digital trail or traffic data created every time each of us sends an e-mail, surfs the Internet, uses a bank card or simply carries a cell phone or text messaging device.[187] [emphasis in original]

---

[186] Barry Cooper, "Privacy and Security in an Age of Terrorism", (October 2004) Fraser Institute Studies in Defence & Foreign Policy Number 3 at 9.

[187] Letter from Office of the Information and Privacy Commissioner (Ontario) to Irwin Cotler April 21, 2005 Regarding Lawful Access Proposals. Online at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16087&N_ID=1&PT_ID=11457&U_ID=0at

The problems examined in *R*. v. *Wise* surrounding the implantation of a tracking device are no longer of much relevance. We enthusiastically carry tracking devices with us from place to place, in our pockets, in our vehicles, we leave an electronic trail behind us wherever we go, like a ghostly electronic doppelganger perpetually frozen in time for so long as a company or organization chooses to retain our electronic records. In order to fully function within this society, we leave a trail, and the onus ought not to be upon us to minimize or eliminate it in order to prevent random monitoring. Before they are able to use such information in an investigation, the authorities ought to be required to show probable cause to do so. Far more so than simple video monitoring, dataveillance is the true panopticon of our digital age.

5.5 Panopticism:

Even in Orwell's classic, 1984, the observation of individuals within that surveillance society is limited by technical factors – there are simply not enough eyes to watch all citizens at all times,[188] rather it was the constant fear of observation by a state apparatus which sought conformity through brutal repression. The fear of observation was enough to ensure general compliance within that regime, as it has within real totalitarian regimes throughout history. This utility of fear of observation and sanction in creating compliance is the theoretical groundwork for Bentham's Panopticon prison design,[189] and Foucault's concept of a panoptic society.[190] In the past, however, technical means were never able to rise above imposing the fear of observation by others. In our technological society, however, CCTV, face recognition software, RFID chips, GPS tracking, and the computerization of currency in the forms of credit and debit cards can create a remarkably complete trail of observation, even in the absence of human intervention, and data mining can be used to ensure that all of this information is at least superficially examined. We have advanced technologically to the point where we have the technical capability to far surpass the level of monitoring described in Orwell's 1984 if we were to so choose. Should it be considered necessary in order to establish complete security, it would be a simple matter of time and money to build a total security infrastructure in which there would no longer be the fear of observation but the absolute certainty of it. The controlling factor would not be fear regarding whether or not one was being watched, because one would be tracked in most of the material aspects of one's life at all times. The controlling factor would become whether the computer program sorting data about one's life were clever enough to detect one's behaviour.

---

[188] George Orwell, *Nineteen Eighty-Four*, (London: Martin Secker & Walberg Ltd., 1949) .

[189] Jeremy Bentham, "Panopticon; or, The Inspection-House: containing the Idea of a New Principle of Construction applicable to Any Sort of Establishment, in which Persons of any Description are to be Kept Under Inspection; and in particular to Penitentiary-Houses, Prisons, Poor-Houses, Lazarettos, Houses of Industry, Manufactories, Hospitals, Work-Houses, Mad-Houses, and Schools: with A Plan of Management Adapted to the Principle: In A Series of Letters, Written in the Year 1787 from Crecheff in White Russia, to a Friend in England," in *The Woks of Jeremy Bentham, Volume Four*, John Bowering, ed. (New York: Russell & Russell Inc., 1962) Pp. 38-66.

[190] Michel Foucault, *Discipline & Punish: The Birth of the Prison* (New York: Vintage Books: 1975.) pp. 195-231.

In actuality, the mere presence of a panoptic system of information gathering in our society is more important than its efficacy for the purposes of producing casual compliance with social norms. Bentham understood the role played by inspection in his regime as one of turning the subject of the inspection into a piece of the machinery of control, ensuring compliance not through external application of force but internalized conformity. "You will please to observe, that though perhaps it is the most important point, that the persons to be inspected should always feel themselves as if under inspection, at least as standing a great chance of being so…"[191] In Foucault's words,

> A real subjugation is born from a fictitious relation. So it is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to observation of the regulations… The efficiency of power, its constraining forces have, in a sense, passed over to the other side – to the side of its surface of application. He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjugation. By this very fact, the external power may throw off its physical weight; it tends to the non-corporeal; and, the more it approaches this limit, the more constant, profound and permanent are its effects: it is a perpetual victory that avoids

---

[191] Jeremy Bentham, "Panopticon; or, The Inspection-House: containing the Idea of a New Principle of Construction applicable to Any Sort of Establishment, in which Persons of any Description are to be Kept Under Inspection; and in particular to Penitentiary-Houses, Prisons, Poor-Houses, Lazarettos, Houses of Industry, Manufactories, Hospitals, Work-Houses, Mad-Houses, and Schools: with A Plan of Management Adapted to the Principle: In A Series of Letters, Written in the Year 1787 from Crecheff in White Russia, to a Friend in England," in *The Woks of Jeremy Bentham, Volume Four*, John Bowering, ed. (New York: Russell & Russell Inc., 1962), p. 44.

> any physical confrontation and which is always decided in advance.[192]

Panopticism on the scale of a building makes all the inmates co-gaolers, panopticism on the scale of a society potentially makes us all into drones of social conformity. If our goal is security and success in eliminating terrorism, crime, or drug trafficking, why not go ahead and complete such a structure, especially if the notion of privacy is so ill defined?

The reason is that a person ought not to live their lives in a fishbowl. The classic dismayed interview with a Hollywood celebrity includes a plea for privacy, and an expression of the tired irony that these celebrities, who have sought attention and approval of others all their lives, can now not go out in public undisguised and unhindered by armies of photographers and tabloid journalists. These celebrities are subject to a constant collection and analysis of their personal information (admittedly many encourage such behaviour in order to maintain their careers) from the products they use to where they live, to their personal relationships, incomes, social life, drug and alcohol use and health status. This information is then broadcast to anyone who will listen for their own enjoyment and the enrichment of advertisers. The general public, of course, is not subjected to such a display of their private lives, but a great deal of information about individuals is already collected. As most people are not famous, and this information never comes to light, they might not feel that they are subjected to constant surveillance, because as far as they can see, nobody is agglomerating the small pieces of personal information which they disclose on a daily basis. No one, so far as they know, is using this information in order to monitor them as an individual.

---

[192] Michel Foucault, *Discipline & Punish: The Birth of the Prison* (New York: Vintage Books: 1975.) , pp. 202-203.

In the case of individuals who are not the centre of a media frenzy like that surrounding celebrities, agglomeration of information might go unnoticed, because the results of that agglomeration are not published and broadcast. This does not make the collection of private information any less real when relating to a private individual, especially when one considers the purpose of this invasion of privacy, which is not to display lurid but essentially unimportant personal details to the public for profit, but to further the application of governmental control of the population. To exercise some level of control over the population is, in fact, the only reason for which a government might collect data about its populace. If there were no desired outcome, there would be no reason to collect the information. Information about income is used to establish and enforce rules on taxation, information about age, diet, activity and the like is used to manage health care, social security and educational resources. If the purpose of government in collecting more information and observing more, or at least having the capacity to do so, is to establish some level of control over the population, what is the public interest in preventing the agglomeration of information and generalized secret observation? Apart from the instinctive reaction which most people raised in the Anglo-American tradition will have against government observation,[193] there are a number of other practical reasons why high levels of security oriented mass observation are not desirable.

The use of technical means to harvest vast amounts of information and process that information is problematic first in that it is devoid of human judgment. A computer algorithm is not capable of understanding the subtleties of human behaviour, and as such is not a good substitute for human observation, yet the only way to process the masses of information which become available through electronic monitoring is through the use of computer analysis. If human based observation were used to sort and analyze all the information which became available through panoptic surveillance, the cost in terms of human resources would be vast, forcing governments to expend tremendous amounts in order to maintain the system. In a sense, the main advancement in technology is not so much in the capacity to collect information about individuals, although that too is increasing, but rather the ability of computerized systems to collate and analyze the information collected in the absence of human intervention, thus leaving the human element of any surveillance system free to concentrate on the pre-sifted intelligence provided by the automated systems. The parallel difficulties presented by this are the false-positive, which is more troubling for individuals being observed, and the false-negative, which is more troubling for the observers.

---

[193] James Q Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty" Yale Law school Public Law & Legal Theory Research Paper Series Research Paper # 64 Pg. 1 Online

In the case of a false positive, an innocent person will come under heightened scrutiny because of the security algorithm which has examined his or her information. For example, individuals with names similar to those used by terror suspects might be pulled aside for additional screening during airport security checks. This problem can be more or less dangerous for individuals depending on the degree of circumspection used by the monitoring organization. It may be as simple as asking a few additional questions in airport security in order to establish the person's true identity[194], but it may be as severe as the case of Khaled El-Masri[195] who alleges that he was detained for months in an Afghan prison by the United States as a terror suspect after having been kidnapped from Germany.

---

http://papers.ssrn.com/abstract=476041 at 2.

[194] As in the case of Edward Allen, a four year old boy on a terrorist watch list, who was detained for additional screening in Huston in December of 2005.

[195] Extrordinary Rendition: Kahlid El-Masti – Statement (2005), Online: American Civil Liberties Union http://www.aclu.org/safefree/extraordinaryrendition/22201res20051206.html .

> It took several months before they concluded he was the victim of mistaken identity, the officials said. His name was similar to an al-Qaeda suspect on an international watch list of possible terrorist operatives, they said.
> By then, Mr Masri, 41, a car salesman from Ulm in Germany, had been flown on a CIA-chartered aircraft to the prison under a secret US program of transferring terrorist suspects from country to country. In prison, Mr Masri said, he was shackled, beaten, photographed nude and injected with drugs by interrogators who pressed him to reveal ties to al-Qaeda.[196]

This sort of example shows us the potential danger of a false positive to the individual involved. Obviously this is an extreme example, but the fact that an innocent person might be kidnapped form the street, flown to a war zone and tortured, all the while allowing his family to believe that he is dead or has deserted them, based on faulty intelligence flouts our traditional belief in the right of the individual to have legal recourse against imprisonment. Until the rights of the individual against non-judicial imprisonment are appropriately guarded, it is in the interests of every individual that their privacy be protected to the greatest degree possible. It is this sort of incident which will cause us to examine, in retrospect, our collective activities as a society during the last several years and feel the shame that has arisen so often before over the treatment of individuals and groups during times of national paranoia. The extrajudicial rendition to torture and other illegal actions taken by our governments in recent times will be remembered in the same way as the internment of Japanese Canadians (and Americans), the anti-communist witch hunts of the 1950s, and other dark periods of our history.

At the root of the problem of the extreme usages of information which cause the dangers of a false positive to be so great is the danger presented to the authorities by the parallel problem of the false negative. These problems are, of course, two sides of the same coin. If the screening system were to fail in a false-negative fashion, and a terrorist attack on the scale of September 11, the Madrid bombings, or the London Underground bombings were to occur, the political repercussions could be terrible. The sense in such cases might be that the current administration was incapable of effectively ensuring security, and that a different administration ought to be established. The political goal for an administration in a time of perceived terrorist crisis can only be the prevention of all terrorist attacks. This goal will tend to lead to the use of extreme measures, morally justified by the potential danger posed by terrorist attacks.

---

[196] "Innocent German Beaten By US Jailers," Sydney Morning Herlad, April 25, 2005, Online:

In reality, it is the nature of the current terrorist problem that eventually, more large scale attacks *will* occur. The main aim of security cannot be to stop all of them, but rather to reduce their numbers and the effectiveness they can hope to achieve. The problem with the automated detection concept is that there must be a more or less specific algorithm in place to operate the sorting of information. If it is too broad, the sorting of information will not be effective enough, and massive demands will be placed upon human resources in further examining data.[197] This would be wasteful, and would potentially reduce the effectiveness of measures over time as a false sense of security overtakes the sense that counterterrorism is a vital pursuit. On the other hand, if sorting algorithms are too narrow, there is a danger that they will not catch their intended targets, and this could allow terrorist attacks to take place unfettered. Security forces are caught in a dilemma wherein they must daily balance the needs of the public to be free from unnecessary harassment, their own needs to meet security goals within current budgets and staffing levels, and protecting

---

http://www.smh.com.au.

[197] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta jr., "Spy Agency Data after Sept.11 Led

against possible large scale and devastating attacks. Electronic data collection is too powerful a tool for security agencies not to seek to use.

Concerted electronic monitoring may be more appropriate in another approach also drawn from drug prohibition. Just as methamphetamine precursors have been placed behind the counter in pharmacies around the country[198], so too should chemicals used in the manufacture of explosives or chemical weapons be controlled and monitored. In this circumstance an ounce of prevention is worth a pound of cure. Since tracking potentially dangerous goods applies surveillance not to individuals but to materials, the degree of privacy invasion is less, and more justifiable. It is worthwhile for authorities to know, for example, who is purchasing ammonium nitrate fertilizer, a precursor to simple explosives frequently used in terrorist attacks. It is much better to be able to track down and investigate a potential bomber prior to the manufacture of an explosive than it is to use CCTV cameras in a transit system to trace the last moments of a bomber and subsequently track their origins as was the case in the London Underground bombings of July 2005.[199] It is better to detect unusual activities surrounding dangerous materials prior to their misuse than to backtrack their path from a terrorist incident, in this way lives can be saved and terrorist organizations might be compromised without the necessity of invading personal privacy on any mass scale. Like the similarly controlled handguns and semi-automatic rifles, these precursors have certain legitimate uses for private individuals (although in this example, the uses of the items used for comparison are primarily recreational) and a

---

F.B.I. to Dead Ends," New York Times, January 17, 2006, online http://www.nytimes.com.

[198] "Retailers to watch sales of meth-making medicines," Globe and Mail, Wednesday, November 2, 2005, Page S2

[199] The suicide bombers on the London Underground in 2005 were captured on CCTV, and their identities and prior movements traced with great speed following the incident. See "Four Suicide Bombers Behind London Tragedy, Police Say," Globe and Mail July 12, 2005. Online: http://www.globeandmail.com

substantial danger of misuse for violent purposes. It is advisable for there to be a tracking database of users of precursor materials, and the potential for at least a cursory investigation regarding the legitimacy of the uses to which they are applied.

There is no perceived need in our society for a massively linked system of fire and smoke detectors in each public and private space within our state linked electronically to fire fighters, although there are some local systems in certain areas, particularly public areas. Instead, we rely upon the public to notice and report such dangers as fire and toxic chemical spills to the appropriate authorities in a timely fashion, and thereby protect the community and individuals within that community. The appropriate model in most areas is not CCTV and dataveillance, but a model like that of fire fighting, a similar model, incidentally, as has served law enforcement for centuries as well. Just as one would not think twice about recognizing it as a civic duty to call the fire department to report a fire, Most of the population, should they be aware of, for example, the purchase of a large quantity of weapons precursors by a person or persons who they cannot see having a need for such materials, would not hesitate to contact the appropriate authorities.

5.6 The Value of Public Anonymity:

Practically, then, there are reasons not to embrace intensive surveillance and dataveillance in our society. The effectiveness of such systems would not justify their expense in terms of resources which might be directed towards other ends, they create an attitude of complacency in the general community and law enforcement, and it would be extremely difficult to establish an appropriate balance between effectiveness and expense. There are other reasons why we might not want to embrace panoptic surveillance which stem from the desire and right of individuals to public anonymity. Rapidly advancing technology will have broad-reaching and fundamental effects on our society, and in order to ensure that they do not eliminate our rights as they have existed for decades or centuries, we must examine what it is that our privacy rights seek to protect. The use of dataveillance to collate massive amounts of otherwise non-secret information about an individual and thereby create a composite portrait of that individual's behaviours, attitudes, tastes, and activities is potentially one of the largest diminutions of privacy ever conceived. The simple act of 'Googling' an individual can disclose a huge amount of information that previously never have been indexed or accessible within practical limits,[200] making each member of society a potential warden in the societal panopticon as well as a subject. At their height of paranoia, the most security minded dictatorships in history could never have collected and analyzed the quantity of information about its subjects as democratic Western countries now have the technological capacity to do to their citizens.

---

[200] Omer Tene, "What Google Knows: Privacy and Internet Search Engines" (2007) online at SSRN.com http://ssrn.com/abstract=1021490 at 7-8.

The greater the ability of technological means to track, record and interpret our movements and behaviour, the less and less we are able to exercise our right to public anonymity. Paul Rosenzweig posits that,

> …what we really must mean by anonymity is not a pure form of privacy akin to secrecy, Rather what we mean… is that even though one's conduct is examined, routinely and regularly, both with and without one's knowledge, nothing adverse should happen to you without good cause.[201]

From this he draws the conclusion that,

> If there are no unjustified consequences (that is consequences that are the product of abuse or error) then, under this vision, there is no effect on a cognizable liberty/privacy interest. In other words, if nobody is there to hear the tree, it doesn't make a sound.[202]

This view of anonymity as simply protecting one from the interference of the authorities is far too narrow. It examines purely practical results rather than seeking the truth of what underlies the need for individuals to maintain their privacy and anonymity. The reasons for a desire for privacy are not simply to avoid government sanction, but to maintain control over one's most personal aspects. The damage caused by an invasion of privacy is not simply in the active results of interference by authorities, but in the diminishment of one's sense of being an autonomous individual actor of value within society.

Constant monitoring in a panoptic system of surveillance affects us in more ways than through the potential application of government sanction, it affects our freedom of expression, because of, "…the fundamental fact that we express private thoughts through conduct as well as through words."[203] The notion that once one is in public he or she is fair

---

[201] Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and Policies for Counter Terrorism* Robert Popp & John Yen, Eds. P 10.

[202] Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and Policies for Counter Terrorism* Robert Popp & John Yen, Eds. P 10.

203 Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to

game for any and all observation by the state simply because passersby might casually observe the individual is simply not tenable because the two types of observation are completely dissimilar. In the one case, there is casual observation by otherwise uninterested parties, which is to be expected any time people come together in society with one another. On the other hand there is deliberate, systematic collection and aggregation of information. Further, the simple absence of a sanction does not establish that the observation of that activity will not have a chilling effect, Solove postulates that "Even surveillance of legal activities can inhibit people from engaging in them."[204] And statistics show the same thing.[205]

> Moreover, data mining aims to be predictive of behavior. In other words, it purports to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity.[206]

With regard to privacy the analogy has arisen in an article by Rosenzwig, "If a tree falls in the forest, does it make a sound," that is to say, "If one's privacy is invaded and no governmental action results, does it make a difference?"[207] Rosenzwig suggests that it does not, that privacy invaded without the knowledge of the individual will not affect society or the individual unless the individual is doing something privately that merits government action. That is not the case. If the populace is watched, they will feel watched, and this will affect their behaviour. It is not through the application of sanctions that our

---

Anonymity", (2002) 72 Mississippi Law Journal 213at 217.

[204] Daniel J. Solove, "'I've got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review, at 17.

[205] Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans" Online at http://dnsi.org/research/Internet/surveryresults.html.

[206] Daniel J. Solove, "'I've got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review, at 18.

[207] Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New

behaviour is changed, through observation, as predicted by Bentham, we become our own censors. Self-censorship will become the norm, and creative and diverse public and private expression will be the victim of a mania for security. An individual is less an individual where he is forced by fear to conform to his own notion of what a good citizen might be in the eyes of the government. The simple absence of sanction is not enough to allow for free use of a medium, "Imagine an online dossier of yourself, residing on the servers of a multinational company, laden with terms such as 'Britney nude,' 'growing marijuana,' 'impotence pills,' 'job search,' 'genital wart,' 'prozac side effects,' 'married gay men,' etc."[208] Where the use of search engines is monitored, the utility of free access to instant information is reduced.

Competing notions of the importance of privacy range from the conceptualization of privacy rights as unaffected where no sanction is enforced, to a broader analysis where invasion of privacy is more similar to the traditional notion of damages in trespassing, where the mere "trampling of the grass" might be actionable.

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.[209]

We see that in Canada, more than in the United States, the notion of a person having a free-standing right to privacy in information that may already have been disclosed to others is embraced by the judiciary. Surely it will be argued that in Canada our

---

Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and Policies for Counter Terrorism* Robert Popp & John Yen, Eds. P 10..

[208] Omer Tene, "What Google Knows: Privacy and Internet Search Engines"2007 online at http://ssrn.com/abstract=1021490 at 12.

[209] *R.* v. *Plant*, [1993] 3 S.C.R. 281.

government would not inspire fear on the part of the citizenry, but the fact of the present government's apparent lack of despotic ambition is no reason to put in place tools which, in the wrong hands, could be used for just such despotic purposes. "Surveillance gives significant power to the watchers. Part of the harm is not simply in being watched, but in the lack of control that people have over the watchers. Surveillance creates the need to worry about the judgment of the watchers."[210] Furthermore, it is not fear of government that will lead to conformity, but shame and embarrassment, and simple self-consciousness. The reason why we, in our form of government, ensure a balance between legislative, executive, and judiciary power, is to ensure that each branch of our government remains bound by law. To abandon the requirement that government be bound by law and held in check by a balance of power is to surrender to any future government's ambition or ill will, and is the height of foolishness. Our constitution must be protected so that it will survive the worst possible case, not simply the good times of accountable and well intentioned government. Our laws must protect us not only in times of peace and plenty, but in times of war, paranoia and insurrection, when we are least able as individuals to see the long term effects of our political actions. We must maintain a principled and rules-based approach to our rights, and not surrender to the notion that our government will always do the right thing or what is best for us all. The great Canadian ideal of Peace Order and Good Government is not an excuse to ignore constitutionalism, but an exhortation to protect constitutionalism even in a time of crisis.

The right to privacy cannot be limited by the mere borders of one's home; privacy and anonymity as against the state are conditions which ought to follow an individual wherever he or she goes unless they are removed by continuing consent or carefully balanced and thoughtful judicial intervention. Prevention of wrongful sanction is one purpose for protecting privacy as against the government and limitation on the government's ability to inquire about its citizens, but it is not the only purpose for or benefit of public anonymity. Rosenweig discards the argument that self-censorship in the context of government scrutiny is likely to result in modification of behaviours which are not specifically prohibited by the government but rather disapproved of by society as a whole because, "…this data set of socially disdained behaviour is exceedingly unlikely to have any relevance to any terrorism investigation."[211] This opinion disregards the powerful non-judicial forces which drive individuals towards conformity, elements of our socialization which would cause an individual to be extremely embarrassed were deviant attitudes or behaviours to be observed. It is not for fear of being arrested that people are not inclined to discuss their sexual behaviour in public, it is due to our desire to maintain privacy despite the fact that we will face no consequences from the government. The mere knowledge that a nameless individual could, without one's consent, examine the minutiae of private matters is disturbing and disruptive of one's sense of self.

---

[210] Daniel J. Solove, "Reconstructing Electronic Surveillance Law," (2004) 72 George Washington Law Review 1701 at 1708.

This attitude also disregards the natural creativity of people regarding new technology. The process called 'function creep' is a phenomenon whereby already existing technology is expanded beyond its originally intended purpose to a new area. Where a powerful tool like data mining exists, it is only a keystroke away from abuse or expansion into new areas of enforcement. Take as an example, the CPIC computer system used by Canadian police to maintain records on criminals and criminal activity, along with motor vehicle and firearms records. This system has been in place for over 30 years, and is an invaluable tool for police, however it is prone to abuse.[212] CPIC is liable to abuse by police officers who seek information about police commissioners or journalists, so would any enhanced technological information collection be liable to abuse by individuals seeking to collect information for their own nefarious purposes. The more advanced and comprehensive the system of data agglomeration, the more tempting its abuse would be.

---

[211] Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and*

Further, this position does not recognize the powerful psychological effect of being watched. Within a modern city, there are few places where one can go for total solitude outside one's own home, and often not there either, depending on one's family situation. One must settle for the anonymity of the public space if one seeks to remove oneself from the society of others. The pleasing effect of being not unobserved but un-remarked upon is the reason why public spaces are an acceptable substitute for total solitude for modern individuals. If one is distinctly observed, however, by electronic eyes or organic ones, the effect is disrupted. A person is not likely to behave freely, nor to feel relaxed if he or she is being stared at. The use of technology is a multiplying effect on the upset caused by staring, "the cyclopean gaze of the camera eye may be equally disquieting, and perhaps more so given the anonymity of the viewer and the unavailability of normal countermeasures, such as staring back or requesting the starer to stop."[213] This effect can only be greater where in addition to camera surveillance there is total panoptic dataveillance.

Policies for Counter Terrorism Robert Popp & John Yen, Eds. at 12.

[212] "Edmonton Police rapped for improper CPIC use," Edmonton Journal, March 8, 2006. online: http://www.edmontonjournal.com

213 Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal 213at 240.

From a young age children are taught that it is not polite to point or stare at others. The reason that it is not polite is that we are made to feel uncomfortable if we are singled out for scrutiny. When on an elevator the typical rider will face the front and watch the numbers light up above the door in order to avoid openly observing others in such an enclosed and densely populated space, so ingrained is our feeling that when in public, one ought to be able to blend into the background of humanity. There is even a thriving but controversial debate in psychology regarding whether the feeling of being watched is actually linked to reality – that is to say, whether our aversion to being stared at is so strong that we can detect staring even where we cannot determine a source of the staring.[214] Such research is inconclusive and controversial, but it does demonstrate that being stared at in our society is so discomforting as to merit such a feeling, and that the feeling is so widespread and universally recognized that it merits scientific study.

Empirical study has been made of the effects of perceived monitoring of Internet activity on Muslim-Americans.[215] This study found that of the Muslim American respondents surveyed, a group that was anticipated to have strong reactions to perceived government surveillance in the post-September 11 environment, only 11.6% had changed their general behaviour after September 11, 2001, and only 8.4% of respondents changed their Internet use. While these numbers regarding an active, conscious change are relatively small, 71.7% believed that the United States Government was monitoring the activities of Muslim-Americans. The difficulty with this survey, and, in fact, any survey of this type is that it relies on self-reporting of changes of behavior consciously adopted by the respondents in the survey, and does not delve into the unconscious reaction to being monitored. Notwithstanding that this survey does not examine subconscious reactions to surveillance, it does show that a substantial portion of Americans have changed their behaviour based on a suspicion that they are being monitored by the government. This effect could only be greater if there was a certainty that they were being monitored. Belief in some kind of monitoring cannot have as strong an effect on behaviour as the certainty of specific types of monitoring. [216]

---

[214] Schmidt S.; Schneider R.; Utts J.; Walach H "Distant intentionality and the feeling of being stared at: Two meta-analyses". (1 May 2004) 95 British Journal of Psychology, no. 2, pp. 235-247

215 Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans" Forthcoming, University of Maryland Law Journal of Race, Religion, Gender and Class, online http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145.

Were one to be aware of constant monitoring by an unblinking, recording, analyzing, computerized eye, the sense of being watched could contribute to similar negative feelings as those caused by intense personal staring. One simply will not behave the same way when one is monitored as when unmonitored. If you believe that the nature of liberty in our society is defined by an absence of interference from and observation by others, especially the state, then such monitoring is a distinct and discomforting practice contributing to the malaise of life in a technological society. Notwithstanding arguments about whether authorities would or would not interfere with the actual activities of individuals engaging in non-illegal practices, a society which is constantly monitored by aloof authorities will be self-censoring, not only in the realm of terrorist activity, but in many areas of activity which are not subject to outright prohibitions. Further, there are economic and social issues that arise where individuals are monitored, for example in the workplace, "Monitored employees are likely to feel less trusted, less motivated, less loyal, and more stressed than employees who are not subject to surveillance."[217] Where this may be an economic drawback to surveillance of the workplace, how much more will the detrimental effects be felt where such surveillance is felt throughout society? The effect that will be seen includes, "… a prevailing climate of suspicion, an increase in adversarial relationships between citizens and government, and an increased tendency to opt out of the official level of society."[218]

---

[216] The psychological effect of mass surveillance is a broad area of study by itself, and is outside the scope of this paper. Any statements made regarding the psychological effect of panoptic surveillance are based on an acceptance of the commonly held attitudes in the literature surrounding panopticism and are not based on psychological research. The oppressive effect of panopticism is an accepted assumption for the purposes of this paper.

Where public appearance and private information are intensely electronically monitored by the state, an individual's freedom to be an individual is diminished.

> The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of public warmth and to become the feelings of everyman. Such a being, although sentient, is fungible; he is not an individual.[219]

Chris Slobogin argues that,

> … in a society that wants to promote freedom of action, camera surveillance… is clearly not an unalloyed good, even if it does significantly reduce crime. People who know that they are under government surveillance will act less spontaneously, more deliberately, less individualistically, and more conventionally; conduct on the streets that is outside the mainstream, susceptible to suspicious interpretation, or merely conspicuous – even if perfectly harmless – will diminish and perhaps even be officially squelched. Some people subject to public camera surveillance, perhaps in particular those from minority

---

[217] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal, 213 at 240.
[218] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal, 213 at 240.
[219] Edward J Bloustein "Privacy as an Aspect of Human Dignity," in *Philosophical Dimensions of Privacy,* F.D. Schoeman Ed. (Cambridge Cambridge University Press, 1984) 156-202 at 188.

> groups, will feel significant anxiety and discomfort although innocent of any crime, and some may react with disdain for government, again despite and probably because of their innocence. Public camera surveillance undermines an open society because it circumscribes unordinary behavior and makes everyone – including the ordinary – more conscious o the government's presence, at least until behavior is suitably conformed and the cameras can be forgotten.[220]

Perhaps it is premature to say that CCTV monitoring and the collection and data mining of tracking data will turn us into a society of Winston Smiths,[221] but certainly it cannot help our sense of individuality to be constantly monitored in the streets by an unblinking electronic eye, or if our every movement is tracked, or if our every purchase or telephone call is recorded centrally and examined for anti-social behaviour. The potential for abuse by individuals and the authorities is too high, and the benefits do not outweigh the drawbacks for purposes of general application. That is not to say, however, that advanced CCTV and intensive electronic monitoring are never appropriate, but their use must be limited and controlled, well known to the public, and justifiable based on a reasonable belief that the absence of such measures will cause real harm to society. In other words, in the race between technology and law, technology is winning.

---

[220] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal, 213 at 245.
[221] Winston Smith is the protagonist of Orwell's classic fiction on panoptic society, 1984.

6.1 Bill C-74 and Proposed Lawful Access Provisions:

In order to deal with advancing technology, the government has sought to change the manner in which monitoring of electronic communications is carried out. This update is certainly due, as communications technology is advancing rapidly, and has been for some time. Little has been done to deal with the policy concerns raised by dataveillance or video surveillance, and "Meaningful legal strictures on government use of public surveillance cameras in Great Britain, Canada, and the United States are non existent."[222] E-mail, instant messaging, cell phone text messaging, voice over Internet, electronic encryption are all concerns for law enforcement seeking to monitor criminal activity. It is important for us to ensure that this updating of the law is carried out in accordance with both respect for privacy and an understanding of the role played by these new technologies. We must remember that there remains a tendency to embrace the notion that the War on Terror constitutes an indefinite emergency, and that, "… in times of fear, government often looks for ways to engage in prevention without being subject to the rigors of the criminal process."[223]

Among the most important developments this area of legislation are the new Lawful Access provisions which were proposed during private stakeholder consultations and partially advanced as Bill C-74 in the final session of the Martin parliament. It is important to delineate the boundaries within which new technology may operate in the pursuit of criminal activity, and in this respect the Lawful Access provisions are a great boon. There is, however, the danger that these provisions open the door for abuse on the part of law enforcement and the diminution of our privacy rights. Bill C-74, had it passed, would have obliged telecommunications service providers to disclose information about their subscribers to authorities without the necessity of a production order, simply on the request of certain law enforcement agents, as well as to construct an infrastructure for the implementation of information gathering on behalf of investigators. These provisions both move some aspects of production orders out of the hands of judicial scrutiny and lay a groundwork for future Lawful Access powers to be implemented

---

[222] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal, 213 at 230.

[223] David Cole, "The New McCarthyism: Repeating History in the War on Terrorism", (2003) 38 Harvard Civil Rights – Civil Liberties Law Review, at 4.

By establishing wide boundaries regarding the application of allegedly non-intrusive technologies, the proposed legislation left open the possibility of function creep and the extension of privacy invasion by technological advancement rather than by judicial or legislative authorization. "Without a normative component, a conception of privacy can only provide a status report on existing privacy norms, rather than guide us towards shaping privacy law and policy in the future."[224] It is indeed a normative component that is needed in dealing with evolving technology. We must decide prior to the development of new technologies what kind of protection we will give to particular kinds of privacy. We must say, for example, that the constant close tracking of the location of an individual's automobile or cellular telephone, or PDA, or convergence device of whatever type, or an individual him or herself, is not an acceptable invasion of privacy without prior judicial authorization on a basis of reasonable grounds to believe that they have committed or will commit a serious crime. As technology develops to provide more and more accurate tracking information regarding an individual based on technological devices that are becoming nearly universal in our society, perhaps even in a retroactive way, the potential for abuse increases tremendously.

The need for legislation controlling the new and rapidly changing area of electronic surveillance through tracking devices and electronic intercepts is not new, and the courts have called for such legislation in the past, for example Justice Cory in *Wise* states,

> I agree with my colleague that it would be preferable if the installation of tracking devices and the subsequent monitoring of vehicles were controlled by legislation. I would also agree that this is a less intrusive means of surveillance than electronic audio or video surveillance. Accordingly a lower standard such as a "solid ground" for suspicion would be a basis for obtaining an authorization from an independent authority, such as a justice of the peace, to install a device and monitor the movements of a vehicle.[225]

But as noted above, the technology available to police during this period (almost twenty years ago, before the common use of GPS and cell phones) was rudimentary and did not allow for nearly the close monitoring and intrusion of modern electronic surveillance. Today, a much more accurate picture of a person's activities can be amassed simply through GPS enables cell phone or PDA, signatures. This enhanced monitoring can take place without the difficulty of implanting a tracking device, as the electronic trail left by most people in our society is so distinct at this point.

Justice La Forrest in his cogent dissent in *Wise* discusses the importance of looking past the current capabilities of a technology and instead concentrating upon the implications of the invasion created by the technology.

> I should note at this point that I am not impressed by the fact that the beeper in this case was a rather unsophisticated device. As we saw, the police with admirable ingenuity were able to track the location of the appellant at all times. But quite apart from this, in this era of explosive technology, can it be long before a device is developed that will be able to track our every movement for indefinite periods even without visual surveillance? ... This is the time to begin

---

[224] Daniel J. Solove, "Conceptualizing Privacy", (2002) 90 California Law Review 1087 at 1142.
[225] *R.* v. *Wise*, [1992] 1 S.C.R. 527 at pp. 548-549.

> regulating the use of electronic tracking devices while they are still in their infancy and before the law enforcement authorities begin routinely using them as part of their work habits.[226]

Today Justice LaForest's dissent seems prescient. We see that tracking technology, particularly through the use of GPS location systems, is much more precise than in the past. Furthermore, the massive success and proliferation of the devices commonly called POS systems, which are used to process credit and debit card transactions electronically, as well as the market dominance of ATMs for banking creates an electronic trail behind an individual which can reveal an enormous amount about an individual's movements in retrospect, or potentially in real time, given some of the provisions of the Lawful Access proposals.[227] It is just this type of expanding and expansive technology which La Forest J. warns against. The dissent in *Wise* is indeed much more reflective of the state of modern technology than the majority decision.

It is good that the previous Canadian government, after an extended period of consultations with stakeholder groups around the country, prepared draft legislation to deal with the relative legal vacuum in which electronic surveillance and tracking exist, beginning with the late session introduction of Bill C-74 just days prior to the collapse of the Liberal minority government. These proposals and outlines illustrated the areas which the bureaucracy believes is important in order to enhance their ability to monitor and control illegal activities in the future. Some of the areas covered by the proposals include requiring telecommunication providers to build in back door surveillance capabilities when establishing or upgrading systems, allowing for reduced evidentiary requirements for gaining access to telecommunications data,[228] criminalizing hacking tools and viruses,[229] requiring the production of electronic tracking data,[230] and transmission data.[231][232] Tracking warrants would be easier to obtain, and their duration would be extended in the case of terrorism and organized crime cases for up to one year without renewal, again based on a reasonable grounds to suspect threshold.[233] To put the new tracking warrants simply, if an individual were simply suspected of links to terrorism or organized crime, the authorities could gain access to a warrant to track all of their electronically traceable locations and a host of other information for one year without further judicial oversight. This would include such things as the GPS location of mobile phones, automobile GPS information, electronic debit and credit transactions, RFID signatures, e-mail and instant message session locations, and would, in fact, give an in depth view of an individual's life for an extended period with minimal judicial oversight.

---

[226] *R.* v. *Wise*, [1992] 1 S.C.R. 527 at 560.
[227] Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations: Criminal Code Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/en/projects-cases/lawful-access/>

The information produced would include where a person was at all times that they carried a cell phone or other traceable electronic device, drove a vehicle with a (more and more common) GPS system or onboard emergency system such as General Motors OnStar, where and when the suspect bought anything with electronic funds transfer, how they paid, and how much they paid, possibly what they bought, and if they do not use electronic payment, where and when they withdraw cash from a bank or bank machine and how much they withdraw. The authorities would be privy to the intimate details of an individual's life for a year with little evidentiary requirement, and minimal judicial supervision. This is well beyond what the public might expect from the authorities. Future mandatory identification cards could contain already available RFID[234] capability which can track movements of identifying tags through the use of detection devices. Even without the inclusion of these devices in identification cards, they are becoming a more and more common inclusion in the packaging or substance of tens of thousands of products. They can be used for inventory tracking, keyless entry to secured areas, even as a substitute for payment by credit card simply by waving a properly programmed tag in front of a scanner. The convenience and low cost of these tags is causing an explosion in their use, and along with them an explosion in the potential tracking data that could be collected.

---

[228] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information,* 1st Sess., 38th Parl., 2005, (1st reading 15 November, 2005).

[229] Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations: Criminal Code Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/en/projects-cases/lawful-access/>, p. 10.

[230] Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations: Criminal Code Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/en/projects-cases/lawful-access/> p. 17.

[231] Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations: Criminal Code Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/en/projects-cases/lawful-access/>, p. 20.

[232] Transmission data is defined in Bill C-74 very broadly, giving rise to the problem that the data sought provides much more information about the communication than a simple telephone record would provide, but retains a low requirement for evidence – that of reasonable grounds to suspect.

[233] Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations: Criminal Code Draft Proposals,* and *Modernizing Investigative Techniques: Proposals,* online: Canadian Internet Policy and

IP addresses and URLs create even deeper problems than those created by the location information disclosed with RFID, GPS and other spatial tracking data.

> With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on. Perhaps even more revealing are URLs. A URL is a pointer. It points to the location of particular information on the Internet... Therefore, URLs can reveal the specific information that people are viewing on the Web. The URL can also contain search terms.[235]

Public Interest Clinic <http://www.cippic.ca/en/projects-cases/lawful-access/>p. 23.

[234] Radio Frequency Identification. This technology is used in areas ranging from the tracking chips placed in pets and cattle to point-of-sale devices to replace barcodes and inventory tracking.

[235] Daniel J. Solove, "Reconstructing Electronic Surveillance Law," (2004) 72 George Washington Law Review 1701 at 1727.

In the case of these pieces of electronic tracking data, the type and scope of information disclosed is huge and potentially intensely personal. It is obvious that such detailed and personal information is of a nature to touch on the "Core of Biographical Information" [236] contemplated by Canadian courts in determining what ought to be protected by privacy law.

Much like certain of the provisions of the Anti-Terrorism Act, the government expects that we as citizens will trust the use of the above-mentioned authority without question. We are assured that any misuse of investigative technologies or powers will be treated seriously by police forces, and that such powers will not be abused either institutionally through the official over extension of the powers granted in the legislation, or individually through the over-zealousness or maliciousness of an individual enforcement officer. The BC privacy commissioner, in response to such suggestions in the consultation process stated

> Assurances that public officials only act in good faith are no substitute for the rule of Law... The assurance at our briefing that, as a practical matter, departments will not give all officers [the power to compel production of subscriber information] is not meaningful. Nor is the assurance that misuse will be punished internally a sufficiently weighty safeguard.[237]

---

236 *R.* v. *Plant*, [1993] 3 S.C.R. 281.

[237] Letter by the BC Privacy Commissioner In Response to 2005 Lawful Access Proposals online at http://www.oipcbc.org/pdfs/public/16763lawfulaccessltr(April8-2005).pdf at p 6.

6.2 Adequacy of complaints-driven monitoring of privacy issues:

The privacy problems raised by proposed Lawful Access provisions are serious because, inter alia, if the authorities conduct themselves in a competent manner, most people whose privacy is invaded by the new provisions will never become aware of what has happened unless criminal charges or at least a police investigation results. For those facing a terrorism investigation who are wrongly investigated the first way that they may become aware of the problem might be when RCMP agents arrive at their door seeking to arrest them without warrant and hold them without charge. The proposed measures adopt a complaint-based mechanism to prevent abuse, but if there is little chance of an individual becoming aware of abuses of the system, there is little value in a complaints based system. Redress through the courts via a Charter challenge or to gain an injunction against surveillance is time consuming, expensive, and outside of the means of most Canadians. Furthermore, there is every likelihood that individuals bringing applications regarding what they suspect to be invasions of privacy (which, as they are secret by nature are liable to be denied by investigators) will be publicly ridiculed as paranoid and delusional, further victimizing the subjects of this privacy invasion.

One of the pillars of privacy legislation around the world has been the concept of informed consent to the collection and storage of information about the individual. Clearly this is not possible in the case of criminal or security investigations, but surely there must be a capacity for individuals to become aware of the problem in order to go forward within a complaint-based system of control. This would not be the case under the proposed regime, as subjects of observation would not even be aware of the secret collection of their data.

> Innocent individuals subject to surreptitious invasions of their privacy may never be in a position to file for, let alone find redress. Any in depth public scrutiny of such matters is the exception to a general rule of secrecy.[238]

During the consultation process, the Department of Justice pointed to a number of safeguards in place, specifically, the Charter of Rights and Freedoms, privacy legislation, the courts, annual reporting to parliament, commission for public complaints against the RCMP, the Security Intelligence Review Committee, and the Privacy Commissioner.[239] The remedy structure however, obviously, cannot include a capacity to retroactively alter the behaviour of the authorities. The best that an individual can hope for is to use these structures, after the fact, to prevent even more difficulty arising from their already difficult situation. In fact, in the absence of a court ruling that certain behaviours will prima facie result in exclusion of evidence, there is little reason for the authorities to respond to criticism in a timely or effective manner when faced with many of these sanctions. One wonders with what seriousness Maher Arar's torturers would have listened to complaints that in the course of his deportation that his privacy concerns were not addressed. The Supreme Court has ruled that analysis after the fact, as in the case of a complaint driven system, would be inadequate.

> … *post facto* analysis would, however, be seriously at odds with the purpose of s. 8. That purpose is, as I have said, to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be

---

[238] Letter from Office of the Information and Privacy Commissioner (Ontario) to Irwin Cotler April 21, 2005 Regarding Lawful Access Proposals. Online at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16087&N_ID=1&PT_ID=11457&U_ID=0 at 5.

[239] Modernizing Investigative Techniques: Overview – online at http://www.cippic.ca/en/projects-cases/lawful-access/Page 6

> accomplished by a system of prior authorization, not one of subsequent validation.[240]

One could argue that there is prior authorization in the case of tracking data where a one-year order is issued based on mere suspicion. This prior authorization of tracking warrants, if it goes forward unchanged from the proposed form, will be among the weakest forms of judicial supervision ever seen in our judicial system, unreasonably weak in relation to the privacy invasion authorized.

In response to these problems within the Lawful Access proposals, the Ontario privacy commissioner has called for the creation of a 'Surveillance and Access Review Agency' an independent, active, and arm's length agency to monitor all Lawful Access applications and investigations, and to provide reporting of these privacy invasions not only to Parliament, but to individuals caught up in the investigation once the danger that such disclosure would disrupt an ongoing investigation has passed. The role of the agency would be to supervise access to personal information, tracking interceptions and warrant applications, monitoring voluntary disclosures to law enforcement, notifying individuals whose privacy has been affected by Lawful Access, and providing information to the government and the public regarding the use of these new powers.[241]

By having an agency which has as its sole responsibility the vetting of Lawful Access requests, Canada could go a long way towards controlling the negative influence that Lawful Access might have in our society. Rather than allowing a subsuming paranoia regarding who or what is being watched and why, this agency could bring these matters into the open in a controlled way, and thereby provide an important brake on the potentially overreaching hand of surveillance while at the same time reassuring Canadians that they will know what their government might be doing to them behind closed doors. They would act as the conscience of the authorities, ensuring that privacy is not trampled upon, but instead tiptoed around, and that individuals who have their privacy invaded have the knowledge required to move forward into the complaints-driven framework of control over Lawful Access. The notion of a government spying on its citizens in a judicial vacuum without any potential for an informed public to respond is anathema to the rule of law, and gives rise to accusations of creeping totalitarianism, which are easily dispersed through a process of openness whereby the public would be aware of the actions of the government. "Transparency is essential to promote accountability and to provide the public with a way to ensure that government officials are not engaging in abuse."[242] Transparency must be the key to any increase in government surveillance powers and to counter-terrorism policy generally.[243]

---

[240] *Hunter et al.* v *Southam Inc.*, [1984] 2 S.C.R. 1421. Para 27.

[241] Letter from Office of the Information and Privacy Commissioner (Ontario) to Irwin Cotler April 21, 2005 Regarding Lawful Access Proposals. Online at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16087&N_ID=1&PT_ID=11457&U_ID=0 at 12.

Transparency, however, is not sufficient. It is important that such an agency have two aspects. First, it must be located outside the investigative and prosecution branch authorities, and, indeed, outside of the executive branch. The role of this body ought to be like that of the auditor general, reporting to the pubic factually without concern for politics or position. Also, reporting to the public, and not just to the public at large but to the particular members of the public who are affected by Lawful Access investigations, on each and every Lawful Access information request that is made, is needed in order to ensure that a complaints-based monitoring system of Lawful Access is a reasonable option.

---

242 Daniel Solove, "Data Mining and the Security-Liberty Debate", (2007-2008) GWU Law School Public Law Research Paper No. 278, 74 University of Chicago Law Review, forthcoming 2008.
at 14.

243 Kent Roach, "National Security, Multiculturalism and Muslim Minorities", (October 2006) University of Toronto Legal Studies Series Research Paper No. 938451 at 33.

It must be inevitable for the person investigated to become aware of the investigation in order to allow him or her to protect their privacy and also their personal security from incorrect data. This body would have the discretion to withhold information regarding an access request provided that they could be satisfied that there was an ongoing investigation, and that disclosing the request would disrupt the investigation, but upon the completion of the investigation disclosure would be made. The onus would be upon the investigative authority which is making the access request to apply for non-disclosure of the request, and to demonstrate on an ongoing basis that the investigation would continue to be threatened by disclosure of the request.

6.3 What controls are necessary for Lawful Access to operate safely and effectively?

What is necessary in order to protect the public in the area of electronic surveillance is openness and transparency? In our society, actions which take place in the public eye are subject to the most important moderating factor in a democratic society, that of the will of an informed public. While the immediate aftermath of 9/11 was an environment of fear and paranoia, we can now look back through the past several years and see that the global crusade and counter-crusade that many imagined as just around the corner is no closer to reality. Calmer voices can begin to prevail, among both the judiciary and the public, recognizing that we can and we must continue our freedoms as we did before, clinging to our way of life as more valuable than total physical safety exercised in a society foreign to our ideals.

At a minimum, safeguards on the invasion of privacy by the government should include a mechanism for the public to become aware of the invasion, and gain access to redress for any wrongdoing. Power exercised in private is liable to lead to abuse. In our society, we demand that power be held accountable as a safeguard against abuse, and it is impossible to hold anyone accountable for the invasion of privacy which occurs in secret and never becomes apparent. Further safeguards which ought to be put into place are an outright ban on holding individuals in secret. A prisoner has no capacity to advocate for him or herself if they are held in secret away from public and judicial scrutiny. Our government must also commit to opposing and attempting to prevent the extrajudicial rendition of Canadians, and use whatever means it can to assist any Canadians who are caught up in an extrajudicial rendition. These areas overlap in their abuse of individual rights to access to justice and protection of the individual. They all remove the opportunity of the individual to object through legal means to their treatment.

One necessity to ensure the appropriate functioning of Lawful Access without unnecessarily abusing rights is an independent agency devoted to ensuring that Lawful Access requests are disclosed in order to protect the public and inform them of the invasions that are being made into their personal information, the stated reasons for the invasion, and the ultimate disposition of the matter, as suggested by the Ontario Privacy Commissioner would establish a technical framework for a rights-respecting Lawful Access regime.

A second necessity is a framework under which the authorities know in pursuit of what crimes or activities they can utilize the more invasive aspects of Lawful Access provisions in order to prevent the creep of these powers into typical investigations. These powers, if they are to be exercised at all, must be exercised as extraordinary powers, not as a typical investigative technique. Monitoring tracking information can have the effect of providing a constant update on the location and communication and economic transactions of an individual, an invasion of privacy if there has ever been one, and this is a powerful tool, which is appropriate in the tool chest of law enforcement only under judicial scrutiny, and on the basis of having a reasonable reason to believe that a serious crime has been or will be committed and that the use of this technique will be appropriate to solve that crime. Basing authorization on suspicion of an individual of any crime of any seriousness could rapidly result in fishing expeditions on individuals who run afoul of the authorities, resulting in a situation where a citizen might be monitored constantly as a form of harassment or as a prophylactic measure against misbehavior, a type of police-imposed probation.

The problem of defining what investigations might legitimately use tracking data is that terrorism is defined so broadly in the Anti-Terrorism Act, and through that act in the

Criminal Code, that a wide array of investigations could use Lawful Access provisions in order to collect information. We must, if we are to include terrorism investigations in the realm of potential Lawful Access applications – which we ought to do – narrow the definition of terrorism used in this context, or add additional criteria to the requirement, such as a requirement that in order to access the more invasive techniques of Lawful Access, the applicant agency would need to demonstrate that there is a reasonable grounds to believe, rather than suspect, an individual of terrorist activity prior to authorization.

The Lawful Access proposals would permit the collection of tracking data based on a lesser standard of proof than that required for most warrant applications. Tracking data, however, is defined as broadly as possible, and the danger is that tracking data will continue to expand in density and content to a point where seeing someone's tracking data is the equivalent of seeing most of their life spread before you on a computer screen. A standard of proof must be established which rises above suspicion for the collection of private information regarding electronic tracking data, much less the content of electronic communications, but more importantly, the type of information which is to be collected ought not to expand along with technological advancement. Are we to be told by legislators that because our credit cards or identity cards contain an RFID tracking device that can monitor our location, that the government is entitled to know our whereabouts at all times with limited if any judicial supervision? It is far more appropriate for the authorities to be required to apply for a warrant based on a reasonable cause to believe standard if they wish to access information that could, for example, disclose all of a person's movements, where a person purchased items or withdrew cash from an ATM, and in what amounts, what websites the person visited and with whom they corresponded. Lawful Access provisions ought to establish a controlled framework for the collection of data based on the type of information the data discloses, rather than the type of data collected. Separate warrants ought to be required for the collection of differing types of data, rather than a blanket warrant for all types of tracking data. It is the agglomeration of the large amount of information provided by 'tracking data' that creates the major privacy concern. The definition of tracking data as it stands is simply too broad and requires categorization based on capability, that is to say, what kind of information is disclosed through the use of the data. In essence, we must establish a system of control over electronic monitoring that bases the grounds for a warrant to apply methods of tracking and information collection on the nature of the information collected, not on the method used. Intercepting private communications ought to be governed by similar rules regardless of the medium. Tracing an individual's location on an ongoing basis ought to be governed by the same rules whether the tracking is done via a primitive directional 'beeper' or the GPS transmitter in a cell phone or the electronic transaction records an individual leaves behind in the course of transacting their day to day business.

Few would suggest that interception or seizure of private communications by the authorities is always inappropriate, few would argue that the police ought never to track the movements of an individual, few would argue that it is never appropriate for authorities to examine with whom certain people are communicating and how. That being said, there must be a balance in our society between the rights of the citizen to be left alone by others - particularly by the government - and the responsibility of government to establish a secure and controlled environment for the public. As it stands now, and as the proposals for Lawful Access come forward, the balance is tipped heavily in favour of governmental scrutiny. Judicial scrutiny of certain investigations will be at a minimum, the average citizen will not have the capacity to effectively dispute the collection of data about them by the state, and advancing technology is outrunning the capacity of legislatures and courts to come to terms with the implications of new technology in a timely manner.

By establishing limitations on the types of investigations that would qualify for the kind of tracking data and communications disclosure contemplated by the Lawful Access provisions, we may take a powerful tool from the arsenal of law enforcement in certain circumstances, but we provide protection for the rights of individuals, which is the essence of security in a democracy. By rejecting the open ended definition of tracking data proposed in the Lawful Access provisions, and instead requiring tight oversight of electronic invasions of privacy in the future, we can more closely control the way in which technology allows the invasion of privacy by government. These limitations, combined with a watchdog organization which can provide timely and meaningful information to the public so as to make the complaints-based scheme workable would go a long way towards protecting privacy, as compared with the provisions as currently suggested.

7.1 Conclusion:

Technology will always be one or more steps ahead in the race between technology and the capacity of the law to protect privacy, unless we change the rules of the race. The only way to remove the multi-year head start of technology is to eliminate technology as a consideration, replacing it with a recognition of the underlying privacy interest regardless of the technology used to investigate. As technology advances, it permits us to place old activities, such as communication, into a new context, such as e-mail or Internet publication. The fundamentals of human existence, however, remain constant. We may change the ways that we communicate and interact with other members of society, but the central aspects of the communication remain the same. Likewise, as technology advances, our integration into a global data network through RFID, GPS and electronic transaction data permit us to be traced with a level of accuracy and completeness that was never before possible. Simply because there is access to such data and information does not mean, however, that unfettered use of that material by government is appropriate. Some argue that within the context of preservation of Western society from extremist terrorism and organized crime, such investigative powers are appropriate, but it is not possible to show that either the seriousness of the threat posed or the effectiveness of the measures taken are appropriate when considered next to the damage to our society that could occur from omnipresent and undisclosed monitoring of the general public.

There is a need for continual judicial oversight of the electronic invasion our privacy, more so now than before terrorism came to the fore as a major concern in our society. Kent Roach and Gary Trotter state that,

> History tells us that the War on Terrorism makes our criminal process more fallible. Common sense suggests that, by fighting what are in reality criminal cases outside of the

> rights-protective criminal process, we exponentially increase the risk of serious miscarriages of justice while at the same time not producing criminal convictions that might be subsequently revealed as wrongful convictions.[244]

And further that, "The courts as bodies committed to precedent and reason have an important role to play in reminding us about our deepest and most lofty commitments in times of crisis."[245] Judicial oversight is not enough, however, where bare minimum constitutional protections leave practical removal of privacy in our society. Government must fashion its laws for information gathering on a fundamental respect for privacy. It is likely that if brought forward as proposed, Lawful Access legislation would past 'constitutional muster' in the courts. This does not mean that we should adopt this standard as that which we will accept from our government in the application of investigative technology.

The ability of courts to intervene for the protection of rights, including privacy rights, must not be thrown off in response to perceived crisis. As technology advances to a point where virtually all of our activities can be monitored to some extent, the temptation on the part of the people is to allow minor invasions of privacy without oversight, or with reduced grounds for invasion, in order to streamline the process of investigation and law enforcement. The temptation to use all the tools at our disposal to ensure security and lawfulness without regard to the potential for abuse must not cause us to abandon the idea that in our society a person is innocent until proven guilty, and that a person's privacy is of inherent value. The need exists regarding privacy in this rapidly changing world to embrace the principle, not the technology, and thereby ensure that a consistent legal framework surrounding privacy will be maintained regardless of technological underpinnings. We cannot change the law fast enough to respond to changing technology, therefore we must attempt to establish laws which will take into account the ever-changing nature of technology and protect our rights regardless of technical capacity. Total panoptic observation is the ultimate weapon in the arsenal of the totalitarian, and a relatively benign security tool in the hands of a libertarian, but once the tool is put in place, who is to say how it will be used in the future? Our system of government was established in post-revolutionary Britain by men who reasonably feared that too much power in the hands of the King would lead to tyranny. They believed that the rule of law was not only for the common man, but for all, including the state. How is our age so different from that in which our system was founded? Technology has advanced, empires have risen and fallen, nationalism has overtaken the divine right of kings and now stands teetering on the verge of what no one knows, but people remain people, power remains power, and leaders remain leaders.

---

[244] Kent Roach and Gary Trotter, "Miscarriages of Justice in the War Against Terrorism", (August, 2005) University of Toronto Legal Studies Series Research Paper No. 04-05, At 71

The difficulty for those leaders is to make the difficult decision to choose options for the enhancement of security that will protect the public both physically from attack by external forces, as well as internally from the very mechanisms designed to protect them This presents a problem.

> Government officials [often] try to do something – the problem is that the "something" they try to do is not the result of an informed and thoughtful policy analysis, but often a cheap gimmicky solution that will grab headlines. The choice for officials is not between doing something or nothing – it is between doing something symbolic versus doing something meaningful but more nuanced and complicated. When it comes to security, the symbolic

---

245 Kent Roach, "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism", (August 2002) 47 McGill Law Journal no 4 893.

> measures often have high civil liberty costs with very little security payoff. Left unexplored are the many more meaningful alternatives where the benefits might outweigh the costs.[246]

The temptation is for the imposition of differential standards of privacy protection where investigation is of differing suspected offences due to a differing expectation of privacy by those engaged in differing proscribed activity, as proposed by Andrew Song "the expectation of privacy that is reasonable should depend on the degree of harm that the government is trying to protect or deter."[247] The problem that this poses is that this throws conceptions of privacy protection into a realm of real and perceived risk, whether physical, as in the case of the risks posed by terrorism, or societal, such as the hazards posed by online sexual predators or drug traffickers. We cannot base a reasonable expectation of privacy on the activity that is suspected, because if we do so any individual suspected of heinous crimes, without the necessity of oversight, will lack the protection of constitutional rights. Protection of privacy rights must not rely on the crime being investigated or the means used to invade the privacy, the use of a reduced evidentiary requirement for obtaining dataveillance warrants is problematic, and while it may not actually violate the Canadian constitution, it would still represent a serious diminution of the private sphere in Canada with little if any tangible benefit.

Many philosophers and statesmen have echoed the sentiment that eternal vigilance is the price of freedom, and it has only rarely been the case that this idea has focused on external threats. It is not by casting our eyes outside, in a search for 'them' or 'they' that we will protect ourselves and our way of life. It is by ensuring, even when 'them' or `they'

---

246 Daniel Solove, "Data Mining and the Security-Liberty Debate", (2007-2008) GWU Law School Public Law Research Paper No. 278, 74 University of Chicago Law Review, forthcoming 2008 at 15.
247 Andrew Song, Technology, Terrorism and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", (May 2003) Harvard Law School Public Law & Legal Theory Research Paper Series no. 73, at 20.

seem to be the greatest danger, that we protect our way of life not only from them but from ourselves and our desire for safety above all else. "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[248] We may well believe, and we may well be right, that in Canada our government has the best of intentions and means us no harm, but surrendering liberties to authority, even where that authority is benevolent, is folly. Islamism, terrorism, communism, fascism, none of these terrors is so powerful as to justify retreating from the establishing principles which have made our society different from those which came before, which is the principle that whether commoner or king we are all bound by the same law, and that the individual is the fundamental unit of our society. Our society has survived worse terrors than it faces today without sacrificing essential liberty. It is our duty to ensure that the sacrifices made by those who have fought and died for our way of life were not in vain and that we will not destroy our own liberties in an attempt to protect ourselves from danger, illusory or otherwise. Such a course will destroy us more completely than any attack from outside our society. Neither bomb nor gun, nor army can harm us more powerfully than the idea that we must fundamentally alter our liberties in order to protect ourselves from danger.

---

[248] Attributed to Benjamin Franklin.

Bibliography

Texts & Treatises

Jeremy Bentham, "Panopticon; or, The Inspection-House: containing the Idea of a New Principle of Construction applicable to Any Sort of Establishment, in which Persons of any Description are to be Kept Under Inspection; and in particular to Penitentiary-Houses, Prisons, Poor-Houses, Lazarettos, Houses of Industry, Manufactories, Hospitals, Work-Houses, Mad-Houses, and Schools: with A Plan of Management Adapted to the Principle: In A Series of Letters, Written in the Year 1787 from Crecheff in White Russia, to a Friend in England," in *The Woks of Jeremy Bentham, Volume Four*, John Bowering, ed. (New York: Russell & Russell Inc., 1962)

Richard K. Betts ed. *Conflict After the Cold War: Arguments on Causes of War and Peace,* (Boston: Allyn and Bacon, 1994).

F.C. DeCoste, *On Coming to Law: An Introduction to Law in Liberal Societies*, (Markham: Butterworths, 2001).

Michel Foucault, *Dicipline & Punish: The Birth of the Prison* (New York: Vintage Books: 1975.).

Michael Ignatieff, *The Lesser Evil: Political Ethics in an Ageof Terror,* (Toronto: Penguin Canada, 2004).

Gilles Kepel, *The War for Muslim Minds: Islam and the West*, (Cambridge: The Belknap Press of the University of Harvard Press, 2004).

George Orwell, *Nineteen Eighty-Four*, (London: Martin Secker & Walberg Ltd., 1949).

Kent Roach, *September 11: Consequences for Canada*, (Montreal: McGill – Queen's University Press, 2003).

Ferdinand David Schoeman Ed. *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984).

Academic Articles

Christopher Bertram, "Afghanistan: A Just Intervention", (2002) Imprints: A Journal of Analytical Socialism, Vol. 6, No. 2 .

Edward J Bloustein, "Privacy as an Aspect of Human Dignity," in Philosophical Dimensions of Privacy, F.D. Schoeman Ed. Cambridge University Press, Cambridge, 1984.156-202.

Robert M. Chesney, "The Sleeper Scenario: Terrorism-support Laws and the Demands of Prevention", (2005) 42 Harvard Journal of Legislation 1.

Sujit Choudhry and Kent Roach, "Racial and Ethnic Profiling: Statutory Discretion, Constitutional Remedies, and Democratic Accountability", (Spring 2003) 41 Osgoode Hall Law Journal no. 1, 1.

David Cole, "The New McCarthyism: Repeating History in the War on Terrorism", (2003) 38 Harvard Civil Rights – Civil Liberties Law Review

David D. Cole, "Security and Freedom – Are the Governments' Efforts to Deal With Terrorism Violative of Our Freedoms?" (2003) Canada-United States Law Journal 29, 339.

Barry Cooper, "Privacy and Security in an Age of Terrorism", (October 2004) Fraser Institute Studies in Defence & Foreign Policy Number 3,

Nina J. Crimm, "Muslim-Americans' Charitable Giving Dillemma: What About a Centralized Terror-Free Donor Advised Fund?" (2008) 13 Roger Williams Law Review, Symposium Issue, Islamic Law ad Law of the Muslim World Research Paper Series at New York Law School no. 08-29.

Alysia Davies, "Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada", (2006) 3 University of Ottawa Law and [Technology Journal, No 1, 249.

Graham E Fuller, "Islamic Fundamentalism", in *Conflict After the Cold War: Arguments on Causes of War and Peace*, Richard K. Betts ed. (Boston: Allyn and Bacon 1994) 386-393.

Malvina Halberstam, "The Evolution of the United Nations Position on Terrorism: From Exempting National Liberation Movements to Criminalizing Terrorism Wherever and by Whomever Committed", (2003) 41 Columbia Journal of International Law no. 3 p. 573.

Kenneth Einar Himma, "Privacy vs. Security: Why Privacy is Not an Absolute Value or Right", online http://ssrn.com/abstract=994458, forthcoming in University of San Diego Law Review.

Seth F. Kreimer, "Rays of Sunlight in a Shadow 'War': FOIA, the Abuses of

Anti-Terrorism, and the Strategy of Transparancy", (2007) 11 Lewis & Clark Law Review :4, 1141.

Bernard Lewis, "Islam and Liberal Democracy: A Historical Overview" (1996) Journal of Democracy 7.2 52-634.

Andrea Locatelli, *Towards Freedom and Democracy. Is Democracy Promotion a Viable Grand Strategy?* (2005) 5 Crossroads n. 1, 5.

Wayne McCormack, "Is it Crime or Is it War? Toward an International Law of Terrorism", University of Utah S.J. Quinney College of Law Legal Studies Research Paper Series Nop. 05-01 http://ssrn.com/abstracts= 747464

Thomas Nagel "Ruthlessness in Public Life " In *Public And Private Morality* Stuart Hampshire ed, (Cambridge: Cambridge University Press, 1977).

Helen Nissenbaum, "Privacy as Contextual Integrity", (2004) 79 Washington Law Review 119.

Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age", (2008), 12 Canadian Criminal Law Review 115.

Wesley W. Pue, "The War on Teror: Constitutional Governance in a State of Permanent Warfare?" (Summer/Fall 2003) 41 Osgoode Hall Law Journal no 2/3 267.

Kent Roach, "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism", (August 2002) 47 McGill Law Journal no 4 893.

Kent Roach, "Sources and Trends in Post- 9/11 Anti-Terrorism Laws" (April 2006) University of Toronto Legal Studies Series Research Paper No XX-06.

Kent Roach, "National Security, Multiculturalism and Muslim Minorities", (October 2006) University of Toronto Legal Studies Series Research Paper No. 938451.

Kent Roach and Gary Trotter, "Miscarriages of Justice in the War Against Terrorism", (August 2005) University of Toronto Legal Studies Series Research Paper No. 04-05.

Paul Rosenzweig, "Privacy and Consequences: Legal and policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty" in *21st Century Enabling Technologies and Policies for Counter Terrorism* Robert Popp & John Yen, Eds. P 10.

Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", (2008) 75 University of Chicago Law Review 261.

Schmidt S.; Schneider R.; Utts J.; Walach H "Distant intentionality and the feeling of being stared at: Two meta-analyses". (May 2004) 95 British Journal of Psychology, no. 2, 235.

Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity", (2002) 72 Mississippi Law Journal 2002, 213.

Daniel J. Solove, "Conceptualizing Privacy", (2002) 90 California Law Review 1087.

Daniel J. Solove, "Reconstructing Electronic Surveillance Law," (2004) 72 The George Washington Law Review 1701 .

Daniel J. Solove, "'I've got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review, 745

Daniel Solove, "Data Mining and the Security-Liberty Debate", (2007-2008) George Washington University Law School Public Law Research Paper No. 278, ,

Andrew Song, "Technology, Terrorism and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", (May 2003) Harvard Law School Public Law & Legal Theory Research Paper Series no. 73,.

David M. Tanovich, "Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention", (Summer 2002) 40 Osgoode Hall Law Journal no. 2 145.

Omer Tene, "What Google Knows: Privacy and Internet Search Engines" 2007 online at http://ssrn.com/abstract=1021490.

K.A. Tripale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd", (2004-2005) Yale Journal of Law & Technology 125.

Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy [The implicit made explicit]" in *Philosophical Dimensions of Privacy* Ferdinand David Schoeman Ed. (Cambridge: Cambridge University Press ,1984) pp. 75-103

James Q Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty Yale Law school Public Law & Legal Theory Research Paper Series Research Paper # 64 (2004) Yale Law Journal # 113 Online http://papers.ssrn.com/abstract=476041

Mary W.S. Wong, "Electronic Surveillance and Privacy in the United States After September 11, 2001: The USA PATRIOT Act" (2002) Singpore Journal of Legal Studies 214.

Jonathan Zittrain, "Searches and Seizures in a Networked World", (2006) 119 Harvard Law Review Forum 83.

Media Articles

"Innocent German Beaten By US Jailers," Sydney Morning Herald, April 25, 2005, Online: http://www.smh.com.au.

"Four Suicide Bombers Behind London Tragedy, Police Say," Globe and Mail July 12, 2005. Online: http://www.globeandmail.com

"Retailers to watch sales of meth-making medicines," Globe and Mail, Wednesday, November 2, 2005, Page S2

"4 Year Old a No-Fly Target," (January 5, 2006) The Globe and Mail online. : http://www.globeandmail.com

"Edmonton Police rapped for improper CPIC use," Edmonton Journal, March 8, 2006. online: http://www.edmontonjournal.com

Rondi Adamson, "Borderless blogs vs. Canada press ban," Christian Science Monitor, April 13, 2005. online, http://www.csmonitor.com.

Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta jr., "Spy Agency Data after Sept.11 Led F.B.I. to Dead Ends," New York Times, January 17, 2006, online http://www.nytimes.com

Andrea Elliott, "To lead the Faithful in a Faith Under Fire," New York Times, (March 6, 2006). Online: www.nytimes.com

Peter Grier, "For telecoms, a storm of lawsuits awaits." May 24, 2006 Christian Science Monitor. Online: www.csmonitor.com

Bernard Lewis, "The Roots of Muslim Rage: Why so Many Mulsims Deeply Resent the West, and Why Their Bitterness Will Not Be Eaily Mollified", The Atlantic, September 1990 v. 266 n 3 p 47.

Paul Koring, "Tracking of calls sparks furor in U.S.: Phone companies gave data to NSA," Globe and Mail May 12, 2006, online www.globeandmail.com.

Paul Koring, "CIA Nominee defends phone-data mining" Globe and Mail, May 15, 2006. online: http://www.globeandmail.com.

Eric Lichtblau, "Libraries Say Yes, Officials Do Quiz them About Users," New York Times, June 20, 2005. online: http://www.nytimes.com.

Charles Mandel, "Internet puts privacy on line: Technology feeds market demand for information about consumers," (January 10, 2006) online. http://www .Canada.com

Dana Priest, "Wrongful Imprisonment: Anatomy of a CIA Mistake", Washington Post (December 4, 2005) online http://www WashingtonPost.com.

Internet Sources

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/index.html

Department of Justice Canada "Lawful Access: Legal Review Follow up consultations: Criminal Code Draft Proposals February-March 2005." http://www.cippic.ca/uploads/JC_CCAmend_2.pdf

Francis Fukuyama, "Has History Restarted since September 11?", nineteenth Annual John Bonython Lecture, Thursday August 8, 2002, Online http://www.cis.org.au/events/jbl/jbl02.htm

Amos N. Guiora, "Legislative and Policy Responses to Terrorism", (August 2005) Case Researh Paper Series in Legal Studies, Working Paper 05-30, online at http://ssrn.com/abstrat=793344

Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans" Online at http://dnsi.org/research/Internet/surveryresults.html.

Judicial Decisions

Cody v. *R.* 2007 QCCA 1276.

Co-Operative Committee on Japanese Canadians et al. v. *Attorney General of Canada et al.* [1947] 1 D.L.R. pp 585-586. (JCPC)

Dagenais v. *Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835

Doe v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

Hunter et al. v *Southam Inc.*, [1984] 2 S.C.R. 1421.

Khawaja v. the *Queen*, 2006 Ont SCJ.

R. v. *A.M.* 2008 SCC 19.

R. v. *Buhay*, [2003] S.C.R. 631.

R. v. *Durate* [1990] 1 S.C.R. 30.

R. v. *Kang-Brown*, 2008 SCC 18.

R. v. *Mann* [2004] 3 S.C.R. 59.

R. v. *Nguyen et al*, 2004 BCSC 76.

R. v. *Oakes*, [1986] 1 S.C.R. 103.

R. v. *Plant*, [1993] 3 S.C.R. 281.

R. v. *Tessling*, [2004] SCC 67.

R. v. *Wise* [1992] 1 S.C.R. 527.

R. v. *Wong*, [1990] 3 S.C.R. 36.

Tele-Mobile Company (a.k.a. Telus Mobility) v. *Ontario*, [2008] SCC 12.

Legislation

Canadian Charter of Rights and Freedoms Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.).

Constitution of Mexico (1917).

"Measures to Prevent International Terrorism which Endangers or Takes Innocent Human Life or Jeopardizes Fundamental Freedoms, and Study of the Underlying Causes of those Forms of Terrorism and Acts of Violence Which Lie in Misery, Frustration, Grievance and Despair and which Cause Some People to Sacrifice Human Lives, Including Their Own, in an Attempt to Effect Radical Changes" G.A res 27/3034, UN GAOR, 27th Sess., Supp No. 30 at 119, U.N. Doc A/RES/27/3034 (1972)

Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information,* 1st Sess., 38th Parl., 2005, (1st reading 15 November, 2005).

Anti-terrorism Act S.C. 2001 c. 41.

Criminal Code, R.S.C. 1985, c. C-46.

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.

Privacy Act, R.S.C. 1985, c. P-21.

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.

War Measures Act, R.S.C. 1927, c 206.

National Emergency Transitional Powers Act, S.C. 1945, c. 25.

Postal Services Act, (U.K.), 2000.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

Other Governmental and NGO documents

Canada's International Policy Statement: A Role of Pride and Influence in the World", 2005.

Canadian Institute for Health Information, "Patient safety in Canada: An Update" August 14, 2007 online www.cihi.ca

Canadian Statistics – *Selected Leading Causes of Death By Sex*, online: <http://www40.statcan.ca/l01/cst01/health36.htm>

"Detention," (2003) online: American Civil Liberties Union http://www.aclu.org/safefree/resources/16828res20030707.html (date accessed, May 20, 2006).

Extrordinary Rendition: Kahlid El-Masti – Statement (2005), Online: American Civil Liberties Union
http://www.aclu.org/safefree/extraordinaryrendition/22201res20051206.html
United States Army Field Manual FMI 3-07.22.
Letter by the BC Privacy Commissioner In Response to 2005 Lawful Access Proposals online at http://www.oipcbc.org/pdfs/public/16763lawfulaccessltr(April8-2005).pdf

Letter from Office of the Information and Privacy Commissioner (Alberta) to Irwin Cotler April 11, 2005 Regarding Lawful Access Proposals. online: http://www.oipc.ab.ca/ims/client/upload/Lawful_Access_April_11_2005.pdf

Letter from Office of the Information and Privacy Commissioner (Ontario) to Irwin Cotler April 21, 2005 Regarding Lawful Access Proposals. Online at: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16087&N_ID=1&PT_ID=11457&U_ID=0

Montreux Declaration, issued at the 27th International Conference of Data Protection and Privacy Commissioners, September 16, 2005.

Speech by the hon. Irwin Cotler, Minister of Justice and Attorney General of Canada on the occasion of an appearance before the Special Committee of the Senate on the Anti-Terrorism Act, Monday, February 21, 2005 Online http://canada.justice.gc.ca/en/news/sp/2005/doc_31398.html

Faisal Kutty and Arsalan Dhirazi, "Canada's Passenger Protect Program: Too Guilty to Fly, Too Innocent to Charge?" Submission by the Canadian Council on American Islamic Relations (CAIR-CAN) on Passenger Protect Program: Identity Screening Regulations to transport Canada, January 31, 2007, online http://ssrn.com/abstract=962797.

Department of Justice Canada, *Lawful Access: Legal Review Follow Up Consultations:Criminal Cose Draft Proposals,* and *Modernizing Investigative Techniques:*

Proposals, online: Canadian Internet Policy and Public Interest Clinic online <http://www.cippic.ca/en/projects-cases/lawful-access/>

Appendix A: List of Acronyms

CBRN – Chemical Biological, Radiological, Nuclear. A reference to particular types of weapons of mass destruction, commonly weapons at which anti-proliferation measures are targeted.

CPIC – Canadian Police Information Centre. A computerized system containing information on criminal records, missing persons and stolen property.

CSIS – The Canadian Security Intelligence Service.

DNS – Denial of Service. An error resulting from an over-loaded website.

FLIR – Forward Looking Infra Red. A type of sensor used from aircraft to find sources of heat such as bodies, vehicle engines and exhausts, and in some cases, marijuana grow operations.

ISP – Internet Service Provider.

LTTE – Liberation Tigers of Tamil Eelam. A Hindu separatist group using suicide bombings and other violent means against the government and people of Sri Lanka.

NSA – National Security Agency. The intelligence agency within the United states Government responsible for intercepting and decoding communications outside of the United States.

PDA – Personal Digital Assistant. A pocket-sized computer used for simple purposes, particularly scheduling.

RFID Chip- Radio Frequency Identification Chip. A small electronic device implanted in many common items which can be scanned and identified with a reader from some distance away.

TSP – Telecommunications Service Provider.

URL – Uniform Resource Locator. A string of characters that represents a location on the Internet.

Appendix B: Definitions

American Gulag Archipelago – A term used by some more inflammatory commentators for a series of more or less secret prisons operated by the United States government outside of its territory. The application of legal and human rights in these prisons is questionable.

Ammonium Nitrate Fertilizer – A chemical fertilizer that is little used in agriculture in most of North America, but which forms a powerful and easy to make explosive when mixed with common chemicals. The resulting explosive is commonly used in mining, and has been used by terrorist groups inside and outside North America.

Asymmetric Political Violence – A blanket term for insurgency, guerrilla warfare and terrorism.

Blackberry – A hand-held communication device that combines telephone, e-mail, text messaging and other features.

Black Site – A location used for the purpose of making an individual disappear from society, usually for interrogation.

Blog – Short for web log. An electronic journal posted on the internet by the user for others to read.

Data Mining – The practice of using powerful computers to sift through vast quantities of personal information in order to seek patterns.

Dataveillance – The use of electronic means to compile personal data about an individual by examining the electronic records left behind by their participation in society.

E-Zine – Electronic Magazine, a type of newsletter forwarded by subscription to users of the internet.

Extraordinary Rendition / Extrajudicial Rendition – The transfer of an individual into the hands of a state's authorities outside the normal deportation or extradition processes.

Googling – Inputting an individual's name into the search engine Google or a similar search engine) and examining the results.

Islamist / Islamism – A term used to describe certain Islamic fundamentalist and Islamic Nationalist movements and the adherents to those movements.

Lawful Access – A term describing a series of proposals brought forward by the Canadian Department of Justice which would establish rules surrounding the use of electronic media for the surveillance of the public.

Panopticon Prison – A proposed prison design which would consist of a series of cells, totally exposed to view from a centralized station which, , in turn, was unobservable to the prisoner, thus creating uncertainty in the mind of the prisoner regarding whether or not he was being watched.

Panoptic Society – A society where monitoring of individuals is so great that each member imposes a strict observance of all rules and norms.

Tracking Data – Data relating to the location of an individual as provided by electronic means such as GPS devices, cell phones, RFID chips and debit and credit card information.

Transmission Data – Data relating to the size, origin, recipient and routing of electronic communications.

Appendix C: Legislative Provisions

Canadian Legislation

Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, (1st Reading 15 November 2005).

11. (1) When a telecommunications service provider installs new software for a transmission apparatus that the service provider operates, the service provider shall meet the operational requirements in respect of that apparatus to the extent that would be enabled by the installation of the software in the form available from the software's manufacturer that would most increase the service provider's ability to meet those operational requirements.

(2) Subsection (1) applies even if the form of the software in question would require the telecommunications service provider to acquire additional software licences or telecommunications facilities to achieve that increased ability.

17. (1) Every telecommunications service provider shall, in accordance with the regulations, provide to a person designated under subsection (3), on his or her written request, any information in the service provider's possession or control respecting the name and address of any subscriber to any of the service provider's telecommunications services and respecting any other identifiers associated with the subscriber.

(2) A designated person shall ensure that he or she makes a request under subsection (1) only in performing, as the case may be, a duty or function

(*a*) of the Canadian Security Intelligence Service under the *Canadian Security Intelligence Service Act*;

(*b*) of a police service, including any related to the enforcement of any laws of Canada, of a province or of a foreign jurisdiction; or

(*c*) of the Commissioner of Competition under the *Competition Act*.

(3) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and the chief or head of a police service constituted under the laws of a province may designate for the purposes of this section any employee of his or her agency, or a class of such employees, whose duties are related to protecting national security or to law enforcement.

(4) The number of persons designated under subsection (3) in respect of a particular agency may not exceed the greater of five and the number that is equal to five percent of the total number of employees of that agency.

(5) The Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service may delegate his or her power to designate persons

under subsection (3) to, respectively, a member of a prescribed class of senior officers of the Royal Canadian Mounted Police or a member of a prescribed class of senior officials of the Canadian Security Intelligence Service.

(6) A designated person shall, with respect to requests made by the person under subsection (1),

(*a*) keep, in accordance with the regulations, a record that
(i) identifies the duty or function referred to in subsection (2) in the performance of which the request is made,

(ii) describes the relevance of the information requested to that duty or function and includes any other information that is necessary to know the reason for the request; and

(*b*) deal with the information provided in response to those requests in accordance with the regulations.

Canadian Charter of Rights and Freedoms **Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, ch. 11 (U.K.).**

1. The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

8. Everyone has the right to be secure against unreasonable search or seizure.

24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

Anti-terrorism Act **S.C. 2001 c. 41.**

1 (*b*) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

(ii) that intentionally

(A) causes death or serious bodily harm to a person by the use of violence,

(B) endangers a person's life,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

Criminal Code **R.S.C. 1985, c. C-46**

Definitions

83.01 (1) The following definitions apply in this Part.

"Canadian"
« Canadien »

"Canadian" means a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act* or a body corporate incorporated and continued under the laws of Canada or a province.

"entity"
« entité »

"entity" means a person, group, trust, partnership or fund or an unincorporated association or organization.

"listed entity"
« entité inscrite »

"listed entity" means an entity on a list established by the Governor in Council under section 83.05.

“terrorist activity” *« activité terroriste »*

“terrorist activity” means

(*a*) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:

(i) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on December 16, 1970,

(ii) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on September 23, 1971,

(iii) the offences referred to in subsection 7(3) that implement the *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*, adopted by the General Assembly of the United Nations on December 14, 1973,

(iv) the offences referred to in subsection 7(3.1) that implement the *International Convention against the Taking of Hostages*, adopted by the General Assembly of the United Nations on December 17, 1979,

(v) the offences referred to in subsection 7(3.4) or (3.6) that implement the *Convention on the Physical Protection of Nuclear Material*, done at Vienna and New York on March 3, 1980,

(vi) the offences referred to in subsection 7(2) that implement the *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, supplementary to the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on February 24, 1988,

(vii) the offences referred to in subsection 7(2.1) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, done at Rome on March 10, 1988,

(viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, done at Rome on March 10, 1988,

(ix) the offences referred to in subsection 7(3.72) that implement the *International Convention for the Suppression of Terrorist Bombings*, adopted by the General Assembly of the United Nations on December 15, 1997, and

(x) the offences referred to in subsection 7(3.73) that implement the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999, or

(*b*) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

(ii) that intentionally

(A) causes death or serious bodily harm to a person by the use of violence,

(B) endangers a person's life,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

"terrorist group"
« groupe terroriste »

"terrorist group" means

(*a*) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or

(*b*) a listed entity,

and includes an association of such entities.

For greater certainty

(1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (*b*) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph.

Facilitation

(2) For the purposes of this Part, facilitation shall be construed in accordance with subsection 83.19(2).

Definition of "judge"

83.28 (1) In this section and section 83.29, "judge" means a provincial court judge or a judge of a superior court of criminal jurisdiction.

Order for gathering evidence

(2) Subject to subsection (3), a peace officer may, for the purposes of an investigation of a terrorism offence, apply *ex parte* to a judge for an order for the gathering of information.

Attorney General's consent

(3) A peace officer may make an application under subsection (2) only if the prior consent of the Attorney General was obtained.

Making of order

(4) A judge to whom an application is made under subsection (2) may make an order for the gathering of information if the judge is satisfied that the consent of the Attorney General was obtained as required by subsection (3) and

(*a*) that there are reasonable grounds to believe that

(i) a terrorism offence has been committed, and

(ii) information concerning the offence, or information that may reveal the whereabouts of a person suspected by the peace officer of having committed the offence, is likely to be obtained as a result of the order; or

(*b*) that

(i) there are reasonable grounds to believe that a terrorism offence will be committed,

(ii) there are reasonable grounds to believe that a person has direct and material information that relates to a terrorism offence referred to in subparagraph (i), or that may reveal the whereabouts of an individual who the peace officer suspects may commit a terrorism offence referred to in that subparagraph, and

(iii) reasonable attempts have been made to obtain the information referred to in subparagraph (ii) from the person referred to in that subparagraph.

Contents of order

(5) An order made under subsection (4) may

(*a*) order the examination, on oath or not, of a person named in the order;

(*b*) order the person to attend at the place fixed by the judge, or by the judge designated under paragraph (*d*), as the case may be, for the examination and to remain in attendance until excused by the presiding judge;

(*c*) order the person to bring to the examination any thing in their possession or control, and produce it to the presiding judge;

(*d*) designate another judge as the judge before whom the examination is to take place; and

(*e*) include any other terms or conditions that the judge considers desirable, including terms or conditions for the protection of the interests of the person named in the order and of third parties or for the protection of any ongoing investigation.

Execution of order

(6) An order made under subsection (4) may be executed anywhere in Canada.

Variation of order

(7) The judge who made the order under subsection (4), or another judge of the same court, may vary its terms and conditions.

Obligation to answer questions and produce things

(8) A person named in an order made under subsection (4) shall answer questions put to the person by the Attorney General or the Attorney General's agent, and shall produce to the presiding judge things that the person was ordered to bring, but may refuse if answering a question or producing a thing would disclose information that is protected by any law relating to non-disclosure of information or to privilege.

Judge to rule

(9) The presiding judge shall rule on any objection or other issue

relating to a refusal to answer a question or to produce a thing.

No person excused from complying with subsection (8)

(10) No person shall be excused from answering a question or producing a thing under subsection (8) on the ground that the answer or thing may tend to incriminate the person or subject the person to any proceeding or penalty, but

(*a*) no answer given or thing produced under subsection (8) shall be used or received against the person in any criminal proceedings against that person, other than a prosecution under section 132 or 136; and

(*b*) no evidence derived from the evidence obtained from the person shall be used or received against the person in any criminal proceedings against that person, other than a prosecution under section 132 or 136.

Right to counsel

(11) A person has the right to retain and instruct counsel at any stage of the proceedings.

Order for custody of thing

(12) The presiding judge, if satisfied that any thing produced during the course of the examination will likely be relevant to the investigation of any terrorism offence, shall order that the thing be given into the custody of the peace officer or someone acting on the peace officer's behalf.

Attorney General's consent required to lay information

83.3 (1) The consent of the Attorney General is required before a peace officer may lay an information under subsection (2).

Terrorist activity

(2) Subject to subsection (1), a peace officer may lay an information before a provincial court judge if the peace officer

(*a*) believes on reasonable grounds that a terrorist activity will be carried out; and

(*b*) suspects on reasonable grounds that the imposition of a recognizance with conditions on a person, or the arrest of a person, is necessary to prevent the carrying out of the terrorist activity.

Appearance

(3) A provincial court judge who receives an information under subsection (2) may cause the person to appear before the provincial court judge.

Arrest without warrant

(4) Notwithstanding subsections (2) and (3), if

(*a*) either

(i) the grounds for laying an information referred to in paragraphs (2)(*a*) and (*b*) exist but, by reason of exigent circumstances, it would be impracticable to lay an information under subsection (2), or

(ii) an information has been laid under subsection (2) and a summons has been issued, and

(*b*) the peace officer suspects on reasonable grounds that the detention of the person in custody is necessary in order to prevent a terrorist activity,

the peace officer may arrest the person without warrant and cause the person to be detained in custody, to be taken before a provincial court judge in accordance with subsection (6).

Duty of peace officer

(5) If a peace officer arrests a person without warrant in the circumstance described in subparagraph (4)(*a*)(i), the peace officer shall, within the time prescribed by paragraph (6)(*a*) or (*b*),

(*a*) lay an information in accordance with subsection (2); or

(*b*) release the person.

When person to be taken before judge

(6) A person detained in custody shall be taken before a provincial court judge in accordance with the following rules:

(*a*) if a provincial court judge is available within a period of twenty-four hours after the person has been arrested, the person shall be taken before a provincial court judge without unreasonable delay and in any event within that period, and

(*b*) if a provincial court judge is not available within a period of twenty-four hours after the person has been arrested, the person shall be taken before a provincial court judge as soon as possible,

unless, at any time before the expiry of the time prescribed in paragraph (*a*) or (*b*) for taking the person before a provincial court judge, the peace officer, or an officer in charge within the meaning of Part XV, is satisfied that the person should be released from custody unconditionally, and so releases the person.

How person dealt with

(7) When a person is taken before a provincial court judge under subsection (6),

(*a*) if an information has not been laid under subsection (2), the judge shall order that the person be released; or

(*b*) if an information has been laid under subsection (2),

(i) the judge shall order that the person be released unless the peace officer who laid the information shows cause why the detention of the person in custody is justified on one or more of the following grounds:

(A) the detention is necessary to ensure the person's appearance before a provincial court judge in order to be dealt with in accordance with subsection (8),

(B) the detention is necessary for the protection or safety of the public, including any witness, having regard to all the circumstances including

(I) the likelihood that, if the person is released from custody, a terrorist activity will be carried out, and

(II) any substantial likelihood that the person will, if released from custody, interfere with the administration of justice, and

(C) any other just cause and, without limiting the generality of the foregoing, that the detention is necessary in order to maintain confidence in the administration of justice, having regard to all the circumstances, including the apparent strength of the peace officer's grounds under subsection (2), and the gravity of any terrorist activity that may be carried out, and

(ii) the judge may adjourn the matter for a hearing under subsection (8) but, if the person is not released under subparagraph (i), the adjournment may not exceed forty-eight hours.

Hearing before judge

(8) The provincial court judge before whom the person appears pursuant to subsection (3)

(*a*) may, if satisfied by the evidence adduced that the peace officer has reasonable grounds for the suspicion, order that the person enter into a recognizance to keep the peace and be of good behaviour for any period that does not exceed twelve months and to comply with any other reasonable conditions prescribed in the recognizance, including the conditions set out in subsection (10), that the provincial court judge considers desirable for preventing the carrying out of a terrorist activity; and

(*b*) if the person was not released under subparagraph (7)(*b*)(i), shall order that the person be released, subject to the recognizance, if any, ordered under paragraph (*a*).

Refusal to enter into recognizance

(9) The provincial court judge may commit the person to prison for a term not exceeding twelve months if the person fails or refuses to enter into the recognizance.

Conditions — firearms

(10) Before making an order under paragraph (8)(*a*), the provincial court judge shall consider whether it is desirable, in the interests of the safety of the person or of any other person, to include as a condition of the recognizance that the person be prohibited from possessing any firearm, cross-bow, prohibited weapon, restricted weapon, prohibited device, ammunition, prohibited ammunition or explosive substance, or all of those things, for any period specified in the recognizance, and where the provincial court judge decides that it is so desirable, the provincial court judge shall add such a condition to the recognizance.

Surrender, etc.

(11) If the provincial court judge adds a condition described in subsection (10) to a recognizance, the provincial court judge shall specify in the recognizance the manner and method by which

(*a*) the things referred to in that subsection that are in the possession of the person shall be surrendered, disposed of, detained, stored or dealt with; and

(*b*) the authorizations, licences and registration certificates held by the person shall be surrendered.

Reasons

(12) If the provincial court judge does not add a condition described in subsection (10) to a recognizance, the provincial court judge shall include in the record a statement of the reasons for not adding the condition.

Variance of conditions

(13) The provincial court judge may, on application of the peace officer, the Attorney General or the person, vary the conditions fixed in the recognizance.

Other provisions to apply

(14) Subsections 810(4) and (5) apply, with any modifications that the circumstances require, to proceedings under this section.

Production order

487.012 (1) A justice or judge may order a person, other than a person under investigation for an offence referred to in paragraph (3)(*a*),

(*a*) to produce documents, or copies of them certified by affidavit to be true copies, or to produce data; or

(*b*) to prepare a document based on documents or data already in existence and produce it.

Production to peace officer

(2) The order shall require the documents or data to be produced within the time, at the place and in the form specified and given

(*a*) to a peace officer named in the order; or

(*b*) to a public officer named in the order, who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

Conditions for issuance of order

(3) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to believe that

(*a*) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;

(*b*) the documents or data will afford evidence respecting the commission of the offence; and

(*c*) the person who is subject to the order has possession or control of the documents or data.

Terms and conditions

(4) The order may contain any terms and conditions that the justice or judge considers advisable in the circumstances, including terms and conditions to protect a privileged communication between a lawyer and their client or, in the province of Quebec, between a lawyer or a notary and their client.

Power to revoke, renew or vary order

(5) The justice or judge who made the order, or a judge of the same territorial division, may revoke, renew or vary the order on an *ex parte* application made by the peace officer or public officer named in the order.

Application

(6) Sections 489.1 and 490 apply, with any modifications that the circumstances require, in respect of documents or data produced under this section.

Probative force of copies

(7) Every copy of a document produced under this section, on proof by affidavit that it is a true copy, is admissible in evidence in proceedings under this or any other Act of Parliament and has the same probative force as the original document would have if it had been proved in the ordinary way.

Return of copies

(8) Copies of documents produced under this section need not be returned.

Information for tracking warrant

492.1 (1) A justice who is satisfied by information on oath in writing that there are reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed and that information that is relevant to the commission of the offence, including the whereabouts of any person, can be obtained through the use of a tracking device, may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(*a*) to install, maintain and remove a tracking device in or on any thing, including a thing carried, used or worn by any person; and

(*b*) to monitor, or to have monitored, a tracking device installed in or on any thing.

Time limit for warrant

(2) A warrant issued under subsection (1) is valid for the period, not exceeding sixty days, mentioned in it.

Further warrants

(3) A justice may issue further warrants under this section.

Definition of "tracking device"

(4) For the purposes of this section, "tracking device" means any device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.

Removal after expiry of warrant

(5) On *ex parte* application in writing supported by affidavit, the justice who issued a warrant under subsection (1) or a further warrant under subsection (3) or any other justice having jurisdiction to issue such warrants may authorize that the tracking device be covertly removed after the expiry of the warrant

(*a*) under any terms or conditions that the justice considers advisable in the public interest; and

(*b*) during any specified period of not more than sixty days.

1993, c. 40, s. 18; 1999, c. 5, s. 18.

Information re number recorder

492.2 (1) A justice who is satisfied by information on oath in writing that there are reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed and that information that would assist in the investigation of the offence could be obtained through the use of a number recorder, may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(*a*) to install, maintain and remove a number recorder in relation to any telephone or telephone line; and

(*b*) to monitor, or to have monitored, the number recorder.

Order re telephone records

(2) When the circumstances referred to in subsection (1) exist, a justice may order that any person or body that lawfully possesses records of telephone calls originated from, or received or intended to be received at, any telephone give the records, or a copy of the records, to a person named in the order.

Other provisions to apply

(3) Subsections 492.1(2) and (3) apply to warrants and orders issued under this section, with such modifications as the circumstances require.

Definition of "number recorder"

(4) For the purposes of this section, "number recorder" means any device that can be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received.

***Freedom of Information and Protection of Privacy Act* R.S.A. 2000 c. f-25,**

(1) (n)"personal information" means recorded information about an identifiable individual, including

(i) the individual's name, home or business address or home or business telephone number,

(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,

(iii) the individual's age, sex, marital status or family status,

(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

(vi) information about the individual's health and health care history, including information about a physical or mental disability,

(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else;

***Privacy Act* R.S.C. 1985 c. p-21**

2. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

British Legislation

***Terrorsm Act* (U.K.), 2000, c 11**

41 Arrest without warrant

(1) A constable may arrest without a warrant a person whom he reasonably suspects to be a terrorist.

(2) Where a person is arrested under this section the provisions of Schedule 8 (detention: treatment, review and extension) shall apply.

(3) Subject to subsections (4) to (7), a person detained under this section shall (unless detained under any other power) be released not later than the end of the period of 48 hours beginning—

(a) with the time of his arrest under this section, or

(b) if he was being detained under Schedule 7 when he was arrested under this section, with the time when his examination under that Schedule began.

(4) If on a review of a person's detention under Part II of Schedule 8 the review officer does not authorise continued detention, the person shall (unless detained in accordance with subsection (5) or (6) or under any other power) be released.

(5) Where a police officer intends to make an application for a warrant under paragraph 29 of Schedule 8 extending a person's detention, the person may be detained pending the making of the application.

(6) Where an application has been made under paragraph 29 or 36 of Schedule 8 in respect of a person's detention, he may be detained pending the conclusion of proceedings on the application.

(7) Where an application under paragraph 29 or 36 of Schedule 8 is granted in respect of a person's detention, he may be detained, subject to paragraph 37 of that Schedule, during the period specified in the warrant.

(8) The refusal of an application in respect of a person's detention under paragraph 29 or 36 of Schedule 8 shall not prevent his continued detention in accordance with this section.

(9) A person who has the powers of a constable in one Part of the United Kingdom may exercise the power under subsection (1) in any Part of the United Kingdom.

***Postal Services Act,* (U.K.), 2000, c.26,**

A

83 Interfering with the mail: postal operators

(1) A person who is engaged in the business of a postal operator commits an offence if, contrary to his duty and without reasonable excuse, he—

(a) intentionally delays or opens a postal packet in the course of its transmission by post, or

(b) intentionally opens a mail-bag.

(2) Subsection (1) does not apply to the delaying or opening of a postal packet or the opening of a mail-bag under the authority of—

(a) this Act or any other enactment (including, in particular, in pursuance of a warrant issued under any other enactment), or

(b) any directly applicable Community provision.

(3) Subsection (1) does not apply to the delaying or opening of a postal packet in accordance with any terms and conditions applicable to its transmission by post.

(4) Subsection (1) does not apply to the delaying of a postal packet as a result of industrial action in contemplation or furtherance of a trade dispute.

(5) In subsection (4) "trade dispute" has the meaning given by section 244 of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992 or Article 127 of the [S.I. 1995/1980 (N.I.12).] Trade Union and Labour Relations (Northern Ireland) Order 1995; and the reference to industrial action shall be construed in accordance with that Act or (as the case may be) that Order.

(6) A person who commits an offence under subsection (1) shall be liable—

(a) on summary conviction, to a fine not exceeding the statutory maximum or to imprisonment for a term not exceeding six months or to both,

(b) on conviction on indictment, to a fine or to imprisonment for a term not exceeding two years or to both.

84 Interfering with the mail: general

(1) A person commits an offence if, without reasonable excuse, he—

(a) intentionally delays or opens a postal packet in the course of its transmission by post, or

(b) intentionally opens a mail-bag.

(2) Subsections (2) to (5) of section 83 apply to subsection (1) above as they apply to subsection (1) of that section.

(3) A person commits an offence if, intending to act to a person's detriment and without reasonable excuse, he opens a postal packet which he knows or reasonably suspects has been incorrectly delivered to him.

(4) Subsections (2) and (3) of section 83 (so far as they relate to the opening of postal packets) apply to subsection (3) above as they apply to subsection (1) of that section.

(5) A person who commits an offence under subsection (1) or (3) shall be liable on summary conviction to a fine not exceeding level 5 on the standard scale or to imprisonment for a term not exceeding six months or to both.

American Legislation

***Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001).**

SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.

Title 18, United States Code, is amended--

(1) in section 2510--
(A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and
(B) in paragraph (14), by inserting `wire or' after `transmission of'; and
(2) in subsections (a) and (b) of section 2703--
(A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR ELECTRONIC' each place it appears;
(B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and
(C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.

SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.

Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended--

(1) by striking `entity the name, address, local and long distance telephone toll billing

records, telephone number or other subscriber number or identity, and length of service of a subscriber' and inserting the following: `entity the--
`(A) name;
`(B) address;
`(C) local and long distance telephone connection records, or records of session times and durations;
`(D) length of service (including start date) and types of service utilized;
`(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
`(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber'; and

(2) by striking `and the types of services the subscriber or customer utilized,'.

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';
(2) by inserting `, routing, addressing,' after `dialing'; and
(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(a) IN GENERAL-

`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.
`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative

officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
`(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--
`(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
`(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
`(iv) any information which has been collected by the device.
To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.
`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'.
(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--
(A) in subparagraph (A)--
(i) by inserting `or other facility' after `telephone line'; and
(ii) by inserting before the semicolon at the end `or applied'; and
(B) by striking subparagraph (C) and inserting the following:
`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.
(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--
(A) by inserting `or other facility' after `the line'; and
(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:
`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.
(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--
(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,

provided, however, that such information shall not include the contents of any communication'; and

(B) by inserting `or process' after `device' each place it appears.

(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--

(A) by striking `of an instrument' and all that follows through the semicolon and inserting `or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and

(B) by inserting `or process' after `a device'.

(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--

(A) by striking `and'; and

(B) by inserting `, and `contents' after `electronic communication service'.

(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.

(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

Other Legislation

Constitution of Mexico (1917)

Article 25. Sealed correspondence sent through the mail shall be exempt from search and its violation shall be punishable by law.